Installing and Upgrading the Avaya S8300 Server

555-234-100
Issue 12
May 2009

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. 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.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

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.

Copyright

Avaya support

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

Contents

About this book

Overview

This document provides procedures to install, upgrade, or migrate an Avaya S8300.

This chapter provides information about the document including: the intended audience, the organization, conventions used, how to get help, and how to download, order, and comment on the document.

Audience

This book is for the following audiences:

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

Using this book

This book is organized into three major sections:

- Section 1: Reference information and hardware installation on page 27
- Section 2: S8300 Server installation and upgrades on page 107
- Section 3: Manual procedures to install and upgrade an S8300 Server on page 205

Section One contains chapters explaining the types of wizards that you can use for installations and upgrades, connection methods, and login methods. These chapters cover:

- Chapter 1: Roadmaps and reference information on page 29
- Chapter 2: Hardware installation for the S8300 Server on page 55

Section Two, in addition to an initial roadmap and top-level tasklist, is organized into five chapters containing installation and/or upgrade scenarios. These scenarios emphasize the use of the Avaya Installation Wizard (IW), Gateway Installation Wizard (GIW). The chapters include:

- Chapter 3: Installing a new S8300 using the Avaya Installation Wizard on page 109
- Chapter 4: Upgrading Communication Manager on an existing S8300B or S8300C Server on page 203

Section Three, in addition to an initial roadmap and top-level tasklist, contains manual procedures to perform the same installation or upgrade scenarios described in Chapters 3 - 7. This section is organized into the following chapters:

- Chapter 5: Manual installation of an S8300 Server on page 207
- Chapter 6: Manual upgrade of an existing S8300B or S8300C to Release 5.2 on page 287
- Chapter 7: Migrating an S8300 Server on page 351

Read Chapter 1: Roadmaps and reference information, before you begin the installation. Chapter 1 contains checklists for the four installation and upgrade scenarios. Then read and follow the procedures in the chapters that apply to the installation or upgrade scenario you are working with.

Read Chapter 2: Hardware installation for the S8300 Server for instructions on installing and cabling the hardware.

Chapter 8 covers the Communication Manager Messaging Application, the INTUITY LX Messaging System, the media gateway sourced announcements, Avaya Integrated Management, the Uninterruptible Power Supply (UPS), Universal Serial Bus (USB) Modems, and other adjuncts.

Conventions

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

Physical dimensions

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

Terminology

- *System* — a general term encompassing all references to the Avaya servers running Communication Manager.
- Circuit pack codes (for example, TN780 or TN2182B) are shown with the *minimum acceptable* alphabetic suffix (like the “B” in the code TN2182B).

  Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every *vintage* of either the minimum suffix or a higher suffix code is necessarily acceptable. A suffix of “P” means that firmware can be downloaded to that circuit pack.
- ASAI — a term synonymous with the newer CallVisor ASAI.
- *UUCSS* — a code that refers to a circuit pack address in cabinet-carrier-slot order.

  nnnVxx is the code that refers to a media module address in gateway-V-slot order.

Recent terminology changes that are important to note include:

- *Communication Manager* — the application that provides call control and the Avaya telephony feature set.

  This application was referred to as *MultiVantage Software* or as *Avaya Call Processing (ACP)* in previous releases. The term *Multivantage* is still used in some CLI commands and in the Web interface. In most of these cases, it is synonymous with *Communication Manager*.
- *Service pack* — a software update.

  This term was often referred to as a *patch* or *update* in previous releases. The terms *update* and *patch* are still used in some CLI commands and in the Web interface. In most of these cases, they are synonymous with *service pack*.
- Communication Manager Messaging - a voice messaging application.

  This application can be installed with the Communication Manager application. It was referred to as Intuity Audix 770 for pre-5.2 releases of Communication Manager.

Typography

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

Commands

- Commands are in **`constant-width bold`** type.

  Example:

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

- Command variables are in ***`bold italic`*** type when they are part of what you must type, and in *plain italic* type when they are not part of what you must type.

  Example:

  Type **`ch ma`** ***`machine_name`***, where *machine_name* is the name of the call delivery machine.

- Command options are in **bold** type inside square brackets.

  Example:

  At the DOS prompt, type **`copybcf`** **[-F34]**.

Keys

- The names of keys are in **bold sans serif** 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.

  Example:

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

System output and field names

- System output and field names on the Web screen are in **bold monospaced type**.

  System output on the CLI screen are in `Courier New type`.

  Example:

  - The system displays the following message:

    The installation is in progress (Web output)

    `The installation is in progress` (CLI output)

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

Downloading this book

You can view or download the latest version of the *Installing and Upgrading the Avaya S8300 Server,* 555-234-100, from the Avaya Web site at http://support.avaya.com. You must have access to the Internet, and a copy of Acrobat Reader must be 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 book. Therefore, the Avaya 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.

Safety labels and security alert labels

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

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

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

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

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

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

Related resources

The CD, *Documentation for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300151, contains a comprehensive library of documents.

For a summary of what is new in the May 2009 release of Communication Manager, see *What's New in Avaya Aura™ Communication Manager, SIP Enablement Services, Avaya Servers and Media Gateways for Release 5.2*, 03-300682.

For more information on the Avaya media gateway and related features, see the following books:

Title	Number
Avaya Aura™ Communication Manager Hardware Description and Reference	555-245-207
Avaya Aura™ Communication Manager Overview	03-300468
Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers	03-300431
Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers	03-300430
Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers	03-300432
Quick Start for Hardware Installation: Avaya S8300 Server and Avaya G700 Media Gateway	555-233-150

Technical assistance

Avaya provides the following resources for technical assistance.

Within the United States

For help with:

- Feature administration and system applications, call the Avaya Technical Consulting - System Support 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
- Security issues, call Avaya Corporate Security at 1-877-993-8442

International

For technical assistance, call the International Technical Assistance Center (ITAC) at +905-943-8801.

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

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.

Documentation

In addition to this book, other description, installation, maintenance, and administration books, and documentation library CDs, are available on Avaya Support Web site, http://support.avaya.com.

.

Sending us comments

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

- Mail, send your comments to:

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

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, *Installing and Upgrading the Avaya S8300 Server,* 555-234-100.

Section 1: Reference information and hardware installation

This section contains chapters explaining the types of wizards that you can use for installations and upgrades, connection methods, and login methods. These chapters cover:

- Chapter 1: Roadmaps and reference information
- Chapter 2: Hardware installation for the S8300 Server

Chapter 1: Roadmaps and reference information

This chapter provides guidance on how to use this book along with connection, login, and other reference information that you will need to perform the installation and upgrade procedures in later chapters.

This Chapter is organized as follows:

- What wizards are available
- About connection and login methods
- About terminal emulation function keys for Communication Manager

What wizards are available

To save time on installations and upgrades, four distinct tools are available for your use:

- Avaya Installation Wizard

  See *Job Aid: Avaya Installation Wizard,* 555-245-754.

- Software Update Manager

  See *Avaya Software Update Manager User Guide,* 14-300168.

  Note:

  These tools replace many normal installation or upgrade procedures described in this document. However, they do not automate all of the tasks associated with an installation or an upgrade. Where a task or tasks must be performed manually, this is noted in subsequent chapters of this document.

Where are the most recent versions of the Wizards

You can find the most recent versions of the Avaya Installation Wizard as well as additional worksheets and job aids for these wizards at http://support.avaya.com/avayaiw.

Tip:

Field- and page-level online help is available with all the wizards.

When to use each wizard

For more detailed information on choosing the right wizard, see *Job Aid: What Provisioning Tools and Wizards Should I Use?,* 555-245-755.

About connection and login methods

This section describes the various ways of connecting to, and logging in to, the Avaya™ S8300 Server. Use this chapter as a reference for the other chapters in this book.

The procedures in this book assume that you are connecting to the S8300 with an Avaya Services laptop. However, the methods apply for any type of PC.

This chapter is organized as follows:

- What physical access methods are available
- Laptop configuration for direct connection to the services port
- About connection methods
- About log in methods

What physical access methods are available

Physical access methods for the S8300. Check for the locations of the following ports:

- If the S8300 is present in the media gateway,
  - Services port in the center of the S8300
  - USB ports on the right side of the S8300

Laptop configuration for direct connection to the services port

There is a special configuration that you need to use for a direct connection to the Services port of the server.

Note:

Avaya Service technicians can use the NetSwitcher program to configure alternate network profiles so they can easily connect to a number of different systems. NetSwitcher configures a profile for each type of system for easy future access without requiring you to reset TCP/IP properties or browser settings manually. NetSwitcher is available from an Avaya Services CTSA.

What network settings are required on the laptop

A laptop connected directly to the Services Ethernet interface on the S8300, S8400, S8500, or S8700-Series Server requires a specific configuration as described in this section.

On any operating system, the network settings need to reflect the following:

- *TCP/IP properties.* Set the laptop's TCP/IP properties as follows:
  - IP address: **192.11.13.5**
  - Subnet mask: **255.255.255.252**
- *Browser settings.* Configure the browser for a direct connection to the Internet. Do *not* use proxies.
- *Server address.* Access the S8300 Server using the URL http://192.11.13.6

The names of the dialog boxes and buttons vary on different operating systems and browser releases. Use your computer's help system if needed to locate the correct place to enter this information.

Configuring the laptop for a direct connection

Set the TCP/IP properties on Windows systems. TCP/IP administration varies among Windows systems.

Note:

Make a record of any IP addresses, DNS servers, or WINS entries that you change when you configure your services computer. Unless you use the NetSwitcher program or an equivalent, you will need to restore these entries to connect to other networks.

To check your version of windows

1. Log in to your laptop, and double-click the **My Computer** icon on your desktop.

   The My Computer window opens.
2. Click **Help** on the My Computer window’s toolbar.

   The Help menu opens and displays the version of Windows installed on your laptop.
3. Follow one of the two procedures below, depending on your operating system.

To change TCP/IP properties and network settings (Windows 2000 and XP)

1. Right-click My Network Places on your desktop or under the Start menu in XP.
2. Select **Properties** to display the **Network and Dial-up Connections** window.

   Windows detects the Ethernet card in your system and created a LAN connection for you. You can see more than one connection.
3. Right-click the correct **Local Area Connection** from the list in the window.
4. Select **Properties** to display the **Local Area Connection Properties** dialog box.
5. Select **Internet Protocol (TCP/IP)**.
6. Click the **Properties** button.

   The **Internet Protocol (TCP/IP) Properties** screen appears.

7. On the General tab, select the radio button **Use the following IP address**. Enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

   Note:

   > Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.
8. Disable DNS service as follows:
   a. Click the radio button labeled **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.

   b. Click the **Advanced** button at the bottom of the screen.

   The **Advanced TCP/IP Settings** screen appears.

   c. Click the **DNS** tab. Verify that no DNS server is administered.

   The **address** field should be blank.
9. Disable WINS Resolution as follows:
   a. Click the **WINS** tab. Make sure WINS is not administered.

   The **address** field should be blank.

   b. Click **OK**.

   If warned about an empty primary WINS address, click **Yes** to continue.
10. Click **OK** twice to accept the address information and close the **TCP/IP** and **Local Area Connection Properties** dialog boxes.
11. Reboot the system if directed to do so.

    After you have made these changes to your computer's network configuration information, the **Network and Dial-up Connections** window shows the status of the **Local Area Connection:**
    - `Enabled` appears when the laptop's Ethernet cable is connected to the server.
    - `Disabled` or unplugged appears if the NIC is not connected to anything.

To change TCP/IP properties (Windows 95, 98, NT 4.0, and Millennium Edition [ME])

1. Access your computer's network information.

   On your desktop:
   - *Windows 95, 98, and NT:* Right-click **Network Neighborhood**.
   - *Windows ME:* Right-click **My Network Places**.
2. Select **Properties** to display the Network dialog box.

3. Locate the TCP/IP properties as follows:
   - *Windows 95, 98, and ME:* On the **Configuration** tab, scroll through the installed network components list to the TCP/IP part of the devices list. Select the TCP/IP device that corresponds to your Ethernet card.
   - *Windows NT:* On the Protocols tab, select **TCP/IP** in the installed network components list.
4. Select the **Properties** button.
5. In the TCP/IP Properties box, click the **IP Address** tab.
6. Click the radio button to **Specify an IP address**.

   Enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

   Note:

   Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.
7. Disable DNS service as follows:
   - *Windows 95, 98, and Me:* Click the **DNS Configuration** tab. Verify that the **Disable DNS** radio button is selected.
   - *Windows NT:* Click the **DNS** tab.
     a. If any IP addresses appear under **DNS Service Search Order**, make a note of them in case you need to restore them later.
     b. Select each IP address in turn and click the **Remove** button.
8. Disable WINS Resolution as follows:
   - *Windows 95, 98, and Me:* Click the **WINS Configuration** tab. Verify that the **Disable WINS Resolution** radio button is selected.
   - *Windows NT:* Click the **WINS Address** tab.
     a. If any IP addresses appear for the Primary and Secondary WINS servers, make a note of them in case you need to restore them later.
     b. Clear each server entry.
     c. Clear the checkbox for **Enable DNS for WINS Resolution**.
9. Click OK twice to accept the address information and close the **Network** dialog box.
10. Reboot the system if directed to do so.

Disabling or bypassing proxy servers in Web browser

If you are connecting a laptop directly to the Services Ethernet interface on the S8300 faceplate, you must either disable or bypass proxy servers as described below.

Note:

The Microsoft Internet Explorer (IE) browser is recommended. If you use IE, it must be version 5.5 or higher. You can use Netscape, but some features of the web interface may not work properly. If you use Netscape, it must be version 6.2 or higher.

To check or change proxy settings

1. Open your Internet browser.
2. Verify that you have a direct connection with no proxies, using one of the following options:
   - **For Internet Explorer:**
     a. Select **Tools > Internet Options**.
     b. Click the **Connections** tab.
     c. Click the **LAN Settings** button.
     d. If **Use a proxy server for your LAN** is not selected, no change is necessary; click **Cancel** to exit.
     e. If **Use a proxy server for your LAN** is selected, you can:
       - Deselect it and click **OK** to exit.

       or,

       - Leave it selected and configure your browser to bypass the proxy server whenever you are connected to the S8300 services port:

         i. Click **Advanced**.
         ii. Type **192.11.13.6** in the Exceptions box. If there are other entries in this box, add to the list of entries and separate entries with a “;”.
         iii. Click **OK** to exit.

- **For Netscape:**

  a. Select **Edit > Preferences**.

  b. Under Category, click **Advanced**.

  c. Click **Proxies**.

  d. If **Direct connection to the Internet** is selected, no change is necessary; click **Cancel** to exit.

  e. If **Direct connection to the Internet** is not selected, you can:

  - select it and click **OK** to exit.

  or,

  - Leave it unselected and configure your browser to bypass the proxy server whenever you are connected to the S8300 services port:

    i. Select **Manual Proxy Configuration** and click **View**.
    ii. Type **192.11.13.6** in the **Exceptions** box (or in the **No Proxy for:** box in later versions of Netscape). If there are other entries in this box, add to the list of entries and separate entries with a ";".
    iii. Click **OK** to exit.

About connection methods

Connecting a laptop to services port of S8300

To connect your laptop directly to the S8300 Server

1. Make sure your laptop meets the hardware and software requirements.
2. Plug an Ethernet crossover cable (MDI to MDI-X) into the 10/100 BaseT Ethernet network interface card (NIC) on your laptop.
   - Crossover cables of various lengths are commercially available.
   - See Table 1 for pinout connections if needed. Crossover of the transmit and receive pairs (as shown) is required.

Table 1: Crossover cable pinout chart

Pin to S8300 Services Port	Connects to	Pin to Laptop Ethernet card
8		8
7		7
6		2
5		5
4		4
3		1
2		6
1		3

3. Connect the other end of the crossover cable to the Services port on the front of the S8300.
4. If your laptop is configured with the correct network settings, you can now open your Internet browser or start an SSH session and log in. When accessing the server from a directly connected laptop, always type the following IP address in the browser's Address or Location field to access the server: **192.11.13.6**

Connecting a laptop to the customer LAN

To connect to the customer’s LAN, either on site or remotely over the Internet, your PC must be assigned an IP address on the LAN. The IP address can be a static address on the customer’s

LAN that you enter in the TCP/IP properties or it can be assigned dynamically with DHCP. Ask the customer how they want you to make the connection.

Connecting an external modem to the S8300 Server

Each S8300 Server requires a Universal Serial Bus (USB) modem for maintenance access and to call out an alarm. The external modem may be connected to the S8300 Server through a universal serial bus (USB) connection, providing dial-up access. The modem type is not optional and must be the specific modem that is shipped with the S8300. Other requirements include:

- The modem requires its own external analog line.
- The remote connection should support a data speed of at least 33.6 Kbps.
- The remote PC must be administered for PPP connections in order to connect through a modem.

A dial-up connection is typically used only for services support of the server, not for routine administration. If the Server is administered to report OSS alarms, it uses the same line for alarm notification. The server cannot report any new alarms while this line is in use.

To set up a dial-up connection

1. Connect one end of the modem's USB cable to an available USB port on the S8300 Server's faceplate. Either USB1 or USB2 (or USB3 on an S8300C or S8300D) can be used.
2. Connect the other end of the cable to the external modem.
3. Connect the modem to an external analog line.

   Note:

   The modem that is shipped with the S8300 obtains its power from the USB interface. There is no power connection.

4. Verify operation as instructed by the modem's documentation.
5. To enable the modem, access the S8300 Server's Maintenance Web Pages (see Logging in to the S8300 Web Interface from your laptop on page 46), and click Enable/Disable Modem on the main menu

   The system displays the Enable/Disable Modem window.

6. Click the radio button for one of the following:
   - Enable modem for one incoming call — use this option if you want to provide one-time access to the server over the modem.
   - Enable modem for unlimited incoming calls — use this option if you want to provide regular dial-up access to the server for Services personnel or some other reason.

The modem is now ready to receive calls.

Setting up Windows for modem connection to the S8300 Server (Windows 2000 or XP)

Note:

The remote dial-up PC must be configured for PPP access.

To set up windows for modem connection to the S8300 server (Windows 2000 or XP):

1. Right-click **My Network Places** and click **Properties**.
2. Click **Make New Connection** and follow the Network Connection Wizard:
3. Select **Dial-up to private network** on the **Network Connection Type** screen.
4. In the **Phone number** field, enter the appropriate telephone number inserting special digits such as 9 and 1 or *70, if necessary.
5. On the **Connection Availability** screen, click **For all users** or **Only for myself**, as appropriate.
6. On the **Completing the Network Connection Wizard** screen, type the name you want to use for this connection. This name will appear in the **Network and Dial-up Connections** list.
7. Check the **Add a shortcut to my desktop**, if desired, and click **Finish**.
8. If a **Connect** screen appears, click **Cancel**.

Configuring the Remote PC for PPP Modem Connection (Windows 2000 or XP, Terminal Emulator, or ASA)

To configure the remote PC for PPP modem connection (Windows 2000 or XP, Terminal Emulator, or ASA):

1. On your PC’s desktop, right-click **My Network Places** and click **Properties**.

   The system deploys the **Network and Dial-up Connections** window.
2. Double click the connection name you made in the previous task, Setting up Windows for modem connection to the S8300 Server (Windows 2000 or XP).

   Note:

   Depending on your system, the **Connect** screen may appear, from which you must select **Properties**.
3. Click the **Security** tab.
4. Select the **Advanced (custom settings)** radio button.
5. Check the **Show terminal window** checkbox.
6. Click the **Networking** tab.

7. In the **Components** box, verify that **Internet Protocol (TCP/IP)** and **Client for Microsoft Networks** are both checked.
8. Select **Internet Protocol (TCP/IP)** and click **Properties**.
9. Click the **Advanced** button.
10. Uncheck (clear) the **Use default gateway on remote network** box.
11. Click **OK** three times to exit and save the changes.

Using Windows for PPP Modem Connection (Windows 2000 or XP)

Note:

To access the system, you may need RAS access and ASG Mobile access.

To use Windows for PPP modem connection (Windows 2000 or XP)

1. Return to the **Network and Dial-up Connections** window and right-click the connection you just created.
2. Select **Connect**.
3. Leave the **User Name**, **Password**, and **Domain** fields blank. If the **Dial** field is blank, enter the appropriate telephone number.
4. Click the **Dial** button. When the S8300 Server's modem answers, the system displays the **After Dial Terminal** window.
5. Log on to the LAN.
    a. Enter your remote access login name and password.
    b. When the **Start PPP Now!** message appears, click **Done**.

    The system displays a small double-computer icon in the lower right portion of your screen.
6. Double click the double-computer icon.
7. The system displays the connection's **Dialup Status** box.
8. Click the **Details** tab.
9. Note the **Server** IP address.
10. Open an SSH session to the S8300 IP address, as noted in the **Dialup Status** box from Step 9.
11. Access SAT or use the CLI commands as needed.

Using Avaya Terminal Emulator for LAN Connection to Communication Manager

If you have the Terminal Emulator installed on your PC, use the following steps to establish a LAN connection to your server. **Note:** the remote dial-up PC must be configured for PPP access.

To use Avaya Terminal Emulator for LAN connection to Communication Manager

1. Double-click the **Terminal Emulator** icon on your desktop. Alternatively, go to the Start menu, select **Programs**, then select **Avaya**, and finally select **Terminal Emulator**. The system displays the Terminal Emulator.
2. From the menu bar at the top of the screen, select **Phones**, then select **Connection List**.

   The system displays the **Connections** window.
3. From the menu bar across the top, select **Connection**, then select **New Connection**.

   The system displays the **Connection Settings** window.
4. Put in a name for the connection. Usually, this will be the name of your S8300 Server.
5. In the **Host** window, click **Telnet**.

   Note:

   > Telnet is turned off by default in Communication Manager. To log in with Telnet, you must turn Telnet on with the Firewall Web page in Communication Manager.
6. Click the **Emulation** tab at the top.

   The system displays the **Emulation** tab.
7. From the Emulator dragdown box, select the emulator you desire, usually 513BCT (default), AT&T 4410, AT&T or DECVT100.
8. In the **Keyboard** window, select **pbx**.
9. Click the **Network** tab.

   The system displays the **Network** tab.
10. In the IP address field, type the IP address of the S8300 Server.
11. In the TCP/IP port number field, leave **23** if you want to log in at the Linux command line. Type **5023** if you want to log in directly to the Communication Manager SAT command line.
12. Click **OK**.

    The **Connection Settings** window disappears.
13. On the **Connections** window, double-click. the name of the connection you just set up.
    - If you used port **5023**, the Login prompt for the Communication Manager software appears.
    - If you used port **23**, the Login prompt for the S8300 Linux software appears.

14. Log in to Communication Manager to access the SAT command prompt screen. If you are logging in as *craft*, you log in to the S8300 Linux software. Then, see Open the Communication Manager SAT Screens on page 50.

Using Avaya Terminal Emulator for Modem Connection to Communication Manager

If you have the Terminal Emulator installed on your PC, use the following steps to establish a modem connection to your server:

To use Avaya Terminal Emulator for Modem Connection to Communication Manager

1. Complete steps 1–8 in To use Avaya Terminal Emulator for LAN connection to Communication Manager on page 42.
2. Click the **Modem** tab.

   The system displays the **Modem** tab.
3. In the IP address field, type the IP address of the connection's **Dialup Status** box as noted in Step 9 in To use Windows for PPP modem connection (Windows 2000 or XP).
4. In the **TCP/IP Port Number** field, leave **23** if you want to log in at the Linux command line. Type **5023** if you want to log in directly to the Communication Manager SAT command line.
5. In the **Modem** field, use the dragdown box to select the type of modem that your PC uses.
6. In the **Serial port** field, select the **COM** port you are using for your modem connection.
7. In the **Baud rate** field, select **9600** from the dragdown box.
8. Click the **Dial Numbers** tab.

   The system displays the **Display Numbers** tab.
9. Type the phone number of the S8300 Server as appropriate. Enter 1 in the **Country Code** field for long-distance.
10. Click **OK**.
11. On the **Connections** window, double-click. the name of the connection you just set up.

    The PC dials up the S8300 Server, and when connected, the login prompt for the Communication Manager software appears.
12. Log in to Communication Manager to access the SAT command prompt screen. If you are logging in as *craft*, you log in to the S8300 Linux software. Then, see Open the Communication Manager SAT Screens on page 50.

About log in methods

This section describes how to log on to the S8300-Series Servers using SSH (Secure Shell), Telnet, or the built-in Web Interface and how to start a SAT session.

These procedures assume:

- You have a crossover cable directly connected from your laptop to the Services port on the S8300 Server, and your laptop is configured for a direct connection.

  or,

- You are connected to the S8300-Series Servers over the customer's LAN, either remotely or on site.

  In this case, your laptop must be configured to connect to the customer's LAN, and you would use the LAN IP address of the S8300 instead of http://192.11.13.6.

Accessing the server's command line interface with SSH

Note:

SSH access is available with Communication Manager releases 2.1 and later.

To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. See Configuring the laptop for a direct connection on page 32. In addition, a third-party SSH client must already be installed on your computer. PuTTY is one such client available for download from http://www.putty.nl/download.html.

Note:

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

⚠ **CAUTION:**

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

To access the command line interface using SSH and PuTTY, perform the following steps:

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

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

2. In the **Host Name (or IP address)** field, type `192.11.13.6` if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.

3. In the **Port** field, type `22`.
4. Under **Protocol**, select **SSH**.
5. In the PuTTY menu on the left, click **Connection > SSH**.

   The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select **2**.
7. In the **Encryption options** window, use the up and down arrows to set **AES (SSH-2)** as the top option and **3DES** as the second option.

   Note:

   > You can also customize the PuTTY tool with other settings, such as for color. For documentation on PuTTY, see http://www.putty.nl/docs.html.
8. Click **Open**.

   Note:

   > If you have not connected to this particular server before, SSH prompts you to accept the server's host key. If you save this key when prompted, you will not be prompted if you connect again later. If you don't save the key, PuTTY prompts you the next time you connect to this server.
   >
   > When connecting though the services laptop interface, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as 192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.
9. If necessary, click **Yes** to accept the server's host key.

   The system displays the **PuTTY** window.
10. Log in as **`craft`**.

Logging in to the S8300 Server from your laptop using Telnet

Telnet is disabled by default in Communication Manager release 4.0 and later. To access the server using telnet, you must enable telnet with either:

- The Firewall Web page in Communication Manager
- The Server Access web page in Communicaton Manager

To run telnet

1. Make sure you have an active Ethernet or serial connection from your computer to the server.
2. Access the telnet program.

   For example:

a. On a Windows system, go to the **Start** menu and select **Run**.

b. Type **telnet 192.11.13.6** to access the S8300 Server CLI.

3. When the **login** prompt appears, type the appropriate user name (for example, *cust* or *craft*).
4. When prompted, enter the appropriate password.
5. If you log in as *craft*, you are prompted to suppress alarm origination.

   Generally you should accept the default value (yes).
6. Enter your terminal type.

   Accept the default value, or enter the appropriate type for your computer. For example, you may use type **ntt**, a terminal type available for Windows NT4.0 or Windows 98. For Windows 2000, use **w2ktt**.
7. If prompted for a high-priority session, typically answer **n**.

   The system displays a prompt. It may take the form <*username@devicename*>.

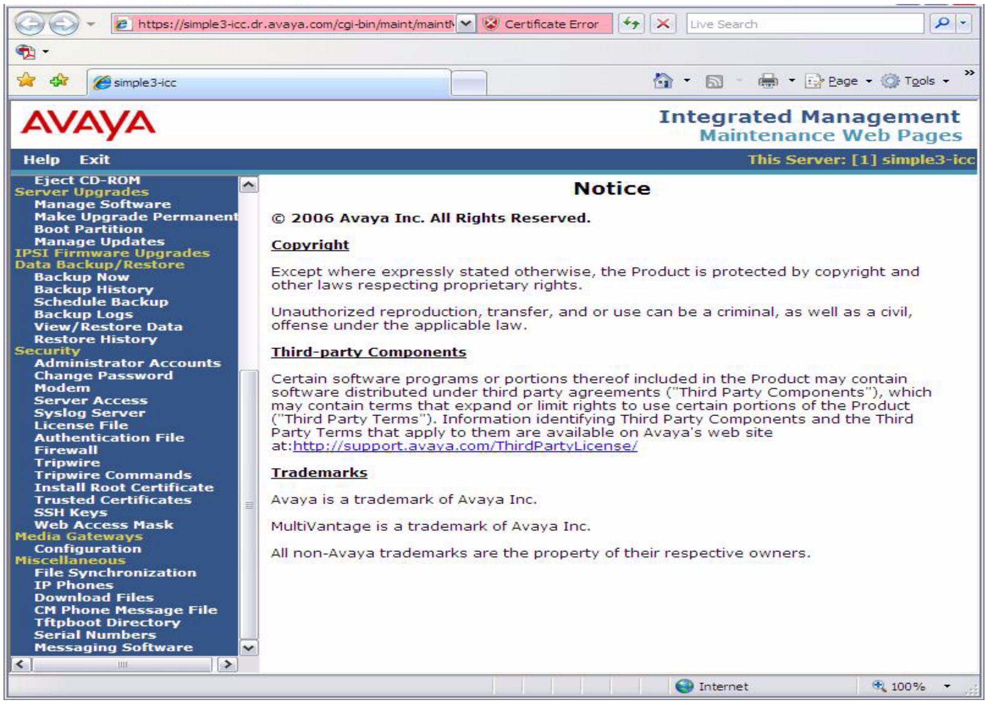
Logging in to the S8300 Web Interface from your laptop

To run the Web Interface

1. Open Internet Explorer (5.5 or later) on your computer.
2. In the Address (or Location) field of your browser, type the **192.11.13.6** (or, for a LAN connection, the IP address of the S8300 Server on the customer LAN) and press **Enter**.

   If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate.
3. The system displays the **Welcome** screen.

Welcome Screen



Notice

© 2006 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:http://support.avaya.com/ThirdPartyLicense/

Trademarks

Avaya is a trademark of Avaya Inc.

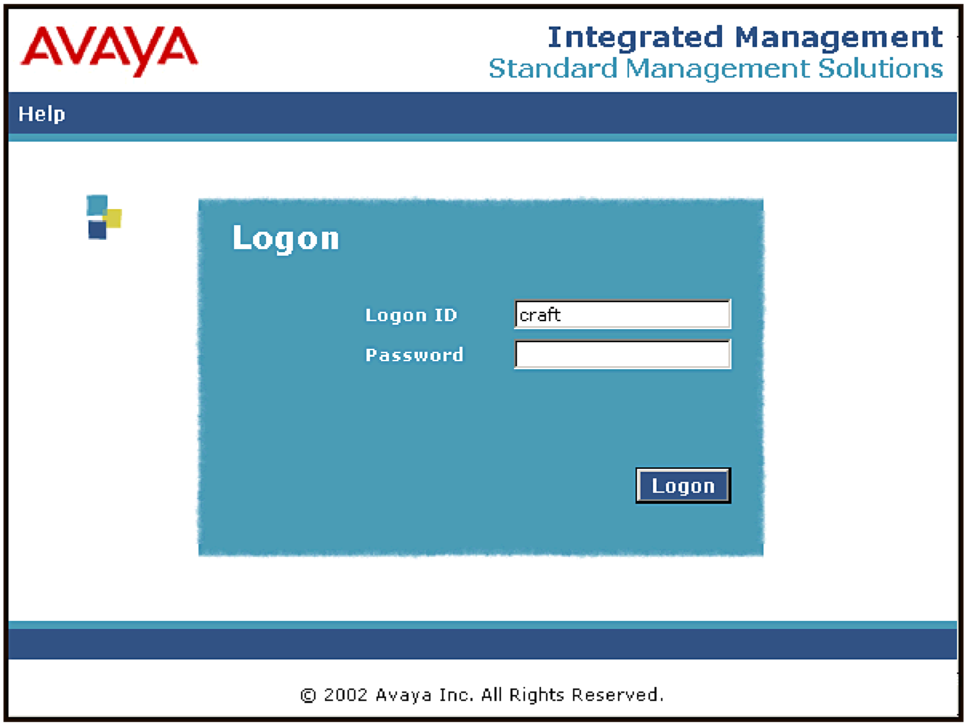
MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

4. Click the **Continue** button.
5. Accept the Client Authentication and Security Certificate to access the **Login** screen.

   The system displays the **Login** screen.

Login Screen


AVAYA
Integrated Management
Standard Management Solutions
Help
Logon
Logon
© 2002 Avaya Inc. All Rights Reserved.

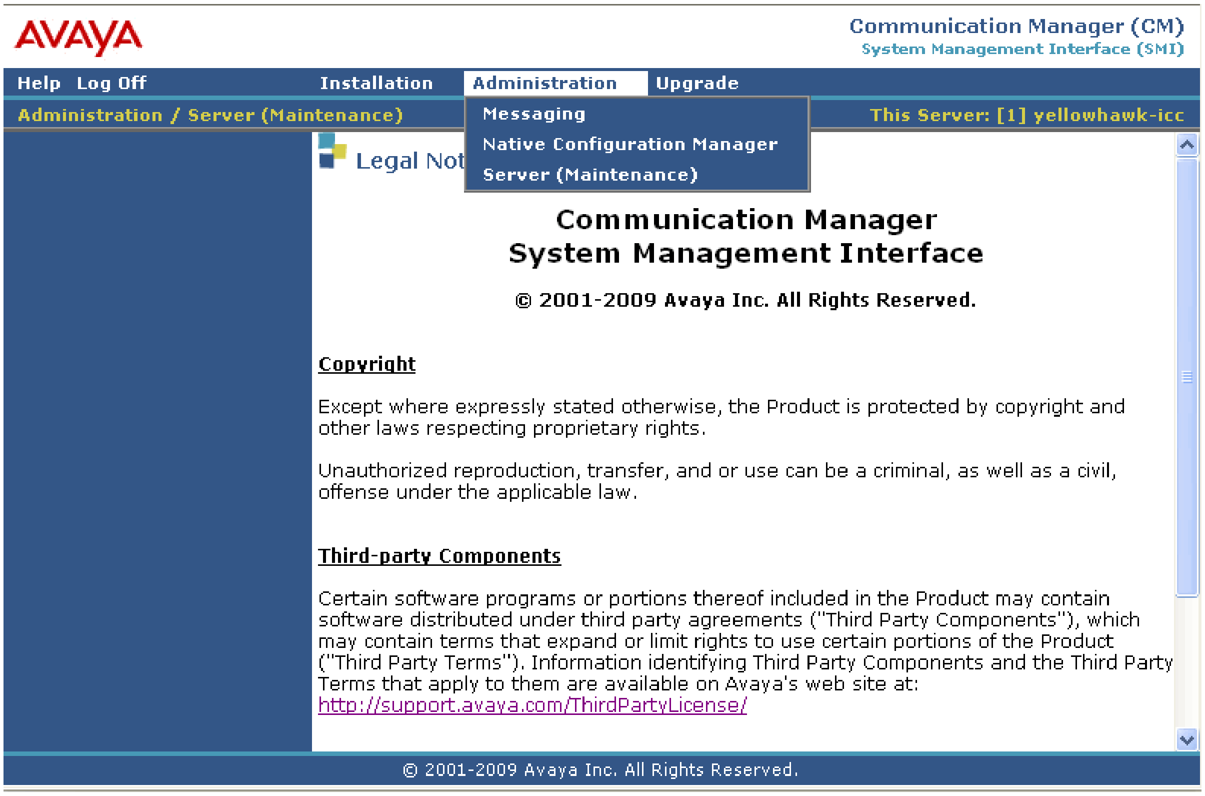
Logon ID: craft

Password:

6. Log in as *craft*.
7. Select **yes** for Suppress Alarm Origination.

   The system displays the main menu for the Integrated Management Suite.

Main Menu


AVAYA
Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
Installation
Administration
Upgrade
Administration / Server (Maintenance)
Messaging
Native Configuration Manager
Server (Maintenance)
This Server: [1] yellowhawk-icc
Legal Not

Communication Manager
System Management Interface

© 2001-2009 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

© 2001-2009 Avaya Inc. All Rights Reserved.

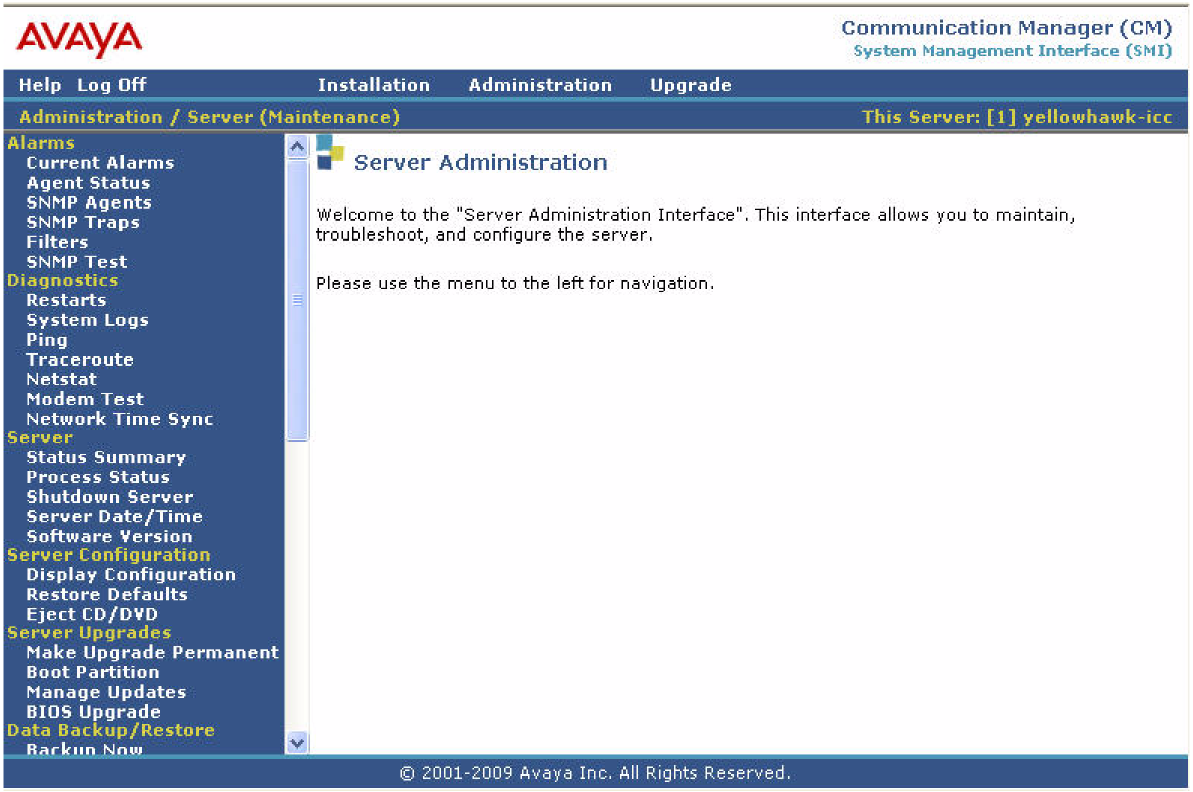
8. (For Communication Manager R5.2 and later) On the **Administration** menu, click **Server (Maintenance)**.

   Note:

   For pre-5.2 releases, click the **Launch Maintenance Web Interface** link on the main page.

   The system displays the S8300 main menu in the left panel and a usage-agreement notice in the right window.

S8300 Main Menu/Usage Agreement Notice



Welcome to the "Server Administration Interface". This interface allows you to maintain, troubleshoot, and configure the server.

Please use the menu to the left for navigation.

9. Check the top of the left panel. Note that:
   - The Avaya Server you are logged into is identified by name and server number.
   - The S8300 Server number is always 1.

Open the Communication Manager SAT Screens

Note:

SSH access is available with Communication Manager releases 2.1 and later.

To run SAT:

1. If you already have a valid SSH session in progress, access the SAT program by typing **sat** or **dsat** at the Linux prompt.

   Or,

   To open SAT directly from your laptop:

   a. Run PuTTY or another SSH client.

   b. Use IP address **192.11.13.6** and port number **5022**.

2. Log in to the Communication Manager as *craft* or *dadmin*.

   Enter your login confirmation information as prompted:

   - *Password prompt*—Type your password in the **Password** field, and click **Login** or press **Enter** again.
   - *ASG challenge*—If the login is Access Security Gateway (ASG) protected, you will see a challenge screen. Enter the correct response and click **Login** or press **Enter**.

3. Enter your terminal type.

   Accept the default value, or enter the appropriate type for your computer. For example, you may use type *ntt*, a terminal type available for Windows NT4.0 or Windows 98. For Windows 2000, use *w2ktt*.

   The system displays the SAT interface.

4. Enter SAT commands as appropriate.

About Avaya Site Administration

A single license for Avaya Site Administration is included with the Standard Integrated Management package.

Configuring Avaya Site Administration

When the Avaya Site Administration software is initially installed on a client machine, it needs to be configured to communicate with Communication Manager on the S8300 Server.

When it runs initially, after downloading, you need to create a new entry for the switch connection. To create new entries for the switch, follow the procedure To add an S8300 switch administration item on page 52.

To add an S8300 switch administration item

1. Click **File > New > Voice System**.

   The system displays the **Add Voice System** window.

2. Enter a name in the **Voice System Name:** field.

   As a technician configuring Avaya Site Administration on your laptop, use a generic name, because you will be able to use this connection name for all S8300 Servers.

3. Click **Next**.

   The **Connection Type** dialog box displays.

4. Click the **Network connection** radio button.
5. Click **Next**.

   The **Network Connection** dialog box displays.

6. Enter the IP address used to connect to the S8300.
7. Click **Next**.

   The **Network Connection/Port Number** dialog box displays.

8. in the **TCP/IP Port Number:** field, type the appropriate port number.

   Use port **23** for the *craft* login. Use port **5023** for the *cust* login.

9. Click **Next**.

   The **Network Connection/Timeout Parameters** dialog box displays. Leave the default values for the timeout parameters.

10. Click **Next**.

    The **Login Type** dialog box displays.

11. Click the “**I want to login manually each time**” radio button.

12. Click **Next**.

    The **Switch Summary** dialog box displays.

13. Check the information.

    Use the **Back** button to make corrections, if necessary.

14. Click the **Test** button to test the connection.
15. When the connection is successfully tested, click **Next** and then **Finish**.

Logging in to the S8300 with ASA

Avaya Site Administration supports a terminal emulation mode, which is directly equivalent to a SAT command interface. Avaya Site Administration also supports other features, including the GEDI and Data Import. For more information refer to the **Online Help**, **Guided Tour**, and **Show Me** accessed from the Avaya Site Administration Help menu.

To start Site Administrator

1. Click **Start** > **Programs** > **Avaya** > **Site Administrator**.
2. Select the switch (server) you want to access.
3. When prompted, log in.
4. When you are logged in, click **Start GEDI**.

About terminal emulation function keys for Communication Manager

When you log in to the Communication Manager SAT screens, your terminal emulation may not display function keys on the screen to help you determine which function keys to press. Use Table 2 as a guide for **ntt** terminal emulation.

Table 2: Key sequences for ntt terminal emulation

Key Sequence		Function Key	Function
ESC	(alpha O) P	F1	Cancel
ESC	(alpha O) Q	F2	
ESC	(alpha O) R	F3	Execute
ESC	(alpha O) S	F4	
ESC	(alpha O) T	F5	Help
ESC	(alpha O) U	F6	Go to Page "N"
ESC	(alpha O) V	F7	Next Page
ESC	(alpha O) W	F8	Previous Page

Table 3 lists key presses for **w2ktt** terminal emulation.

Table 3: Key sequences for w2ktt terminal emulation

Key Sequence		Function Key	Function
ESC	x	F1	Cancel
ESC		F2	
ESC	e	F3	Execute
ESC		F4	
ESC	h	F5	Help
ESC		F6	
ESC	n	F7	Next Page
ESC	p	F8	Previous Page

Chapter 2: Hardware installation for the S8300 Server

The chapter is organized in two main sections:

- About hardware components - Describes the S8300 components.
- Inserting the Avaya S8300 Server (if necessary for standalone service or LSP) - Provides hardware installation and cabling procedures.
- Terminal server installation - Provides information on connecting an adjunct equipment to a G700 with an S8300 Server.

Note:

See *Quick Start for Hardware Installation: Avaya S8300 Server and Avaya G700 Media Gateway*, 555-233-150, for an overview of the S8300 hardware.

About hardware components

This section describes the components of an Avaya S8300-Series Server.

What are the functions of the S8300 LED Indicators

There are a set of LED indicators on the faceplate of the S8300. A shutdown button is also on the faceplate, which when depressed for about three seconds, will shut down the system, including the operating software on the S8300. The LED flashes when shutdown is in progress and remains on steady when it is safe to remove the S8300 or to power down.

The functions of the S8300 LEDs are:

- The red ALM LED on the S8300 is off when the system is operational unless a Major Alarm has been raised. **For an S8300C** or **S8300D Server**, during the BIOS boot, the ALM LED is on (not flashing). When the BIOS boot finishes, the ALM LED starts flashing to indicate that all hardware diagnostics have passed and the system is ready to load the OS. The ALM LED continues to flash until the Avaya software is installed. The ALM LED turns off when the Avaya Linux drivers are installed.

  Note:

  The BIOS boot LED flashes during the whole software installation, through rebooting, since the system is not running from the Avaya software yet.

- The green APP (S8300C or S8300D) or TST (S8300B) LED on the S8300 (primary controller or LSP) is on when Communication Manager is running.
- The yellow ACT LED on the S8300 is on whenever a media gateway, an IP telephone, or an IP console is registered with the S8300. It is off when none of these IP endpoints are registered.
- The green OK-to-Remove LED on the S8300 indicates that shutdown is complete and that it is safe to remove the server or power down the system.

  When the S8300 is a local survivable processor (LSP), no LEDs will be lit during normal operations. In case of a network failure or loss of contact with the primary S8300 (or S8500 or S8700-series Server), the media gateway registers with the LSP. At that time, the red Alarm LED will light.

When you first power up the S8300, the red Major Alarm LED lights. During startup, an LED sequence runs: red ALM, green APP (S8300C or S8300D) or TST (S8300B), yellow ACT, green OK-to-Remove, and the three LEDs under the Services Port, after which all LEDs turn off. At this point, you can connect to the S8300. When Communication Manager starts, the green APP LED turns on and stays on.

What is the S8300 Server

The S8300 Server is an Intel processor complex that mounts in one of the media module slots depending on the media gateway. For example, S8300 Server mounts in the first media module slot (V1) of the G450 Media Gateway. The S8300 Server has:

- Communication Manager (For a full description see: http://www.avaya.com/support)
- Administration and maintenance provisioning software

- (**S8300B model only**) 20 or 30 GB hard drive
  (**S8300C model only**) 40 GB hard drive

  (**S8300D model only**) 160 GB hard drive
- (**S8300B model only**) 512 MB RAM (in two 256 MB DIMM strips)
  (**S8300C model only**) 1 GB RAM (with one 1 GB DIMM)

  (**S8300D model only**) 8 GB DRAM
- Web server
- Linux OS (Red Hat)
- Support of H.248 and H.323 Protocols
- TFTP server and other IP services
- (**S8300C or S8300D Server only**) Internal compact flash drive, which is used as the primary reboot device and provides additional reliability.

  Note:

  The current versions (B and C) of the S8300 are backward compatible with the previous (A) version. The A version has a 20 G hard drive and 256 MB RAM.

What is a Local Survivable Processor (LSP)

The S8300 Server can act as a survivable call-processing server for remote or branch customer locations. As an LSP, the S8300 Server carries a complete set of Communication Manager features, and its license file allows it to function as a survivable call processor. If the link between the remote media gateways and the primary controller is broken, those telephones and media gateways that are designated to receive backup service from the LSP will register with the LSP. The LSP is in a license error mode while it provides control to any devices (see *Avaya Aura™ Communication Manager Hardware Description and Reference,* 555-245-207).

About endpoint and adjunct components

Additional components and adjunct systems provide sets of tools that allow the customer to obtain the best possible performance.

Other components and adjunct systems that make up the S8300 Server with a media gateway include:

- Analog phones and fax machines
- DCP phones
- IP phones
- IP Softphones
- LAN Ethernet switches
- Avaya Integrated Management

- INTUITY AUDIX LX Messaging System
- Communication Manager Messaging
- ASAI Co-Resident DEFINITY LAN Gateway (DLG)
- Call Center
- Uninteruptible Power Supply (UPS)
- Universal Serial Bus (USB) Modems
- USB Compact Flash device (S8300C, S8300D only)
- DVD/CD-ROM drive

Who needs a Single Sign-On (SSO) authentication login

You should obtain a personal Single Sign-On (SSO) for Remote Feature Activation (RFA) web site authentication login before going to the site for installation. You must complete the authentication process before you can be assigned an SSO authentication login.

As a first-time user:

- Business Partners should point their browsers to the Business Partner portal option sales_market, services-voice, training tools and procedures to select RFA (or go directly to: http://rfa.avaya.com).
- Associates should point their browsers to the Avaya Associate portal (or go directly to: http://rfa.avaya.com).
- Contractors should point their browsers to Avaya.com (or go directly to: http://rfa.avaya.com).

From that point, log into SSO and complete the process to obtain your personal login.

Reviewing demarcation points and connectivity for the Communication Manager Messaging

A demarcation point defines the extent of Avaya's responsibilities for a product. Beyond this point, the customer is responsible for providing overall service. Generally, Avaya is responsible for all Avaya-provided equipment.

The demarcation point for the Communication Manager Messaging Application is the S8300 Server ethernet ports. The customer is responsible for ensuring that the following items are correct and functioning normally:

- The LAN cable and connector used to connect to the S8300 Server
- LAN administration outside of the Avaya equipment
- Maintaining the TCP/IP addresses and administration on the S8300 Server after installation, unless otherwise specified by contract

- Valid IP address, subnet mask, and gateway information for administration on the S8300 Server

Avaya service technicians who are dispatched for installing Communication Manager Messaging system application are not responsible for troubleshooting the LAN.

Maintaining system security

Remember that security is important.

To protect password security, ensure that the following precautions are followed:

- Change the passwords for the system administrator (sa), voice mail administrator (vm), and dadmin logins before you begin the verification and acceptance of the Communication Manager Messaging software.
- Do not leave written passwords in a place where they are accessible by others.
- At the first opportunity, privately give the passwords to the customer’s designated representative.
- If you suspect that the security of any password has been compromised, immediately notify your project manager or system administrator.

Verifying features for the Communication Manager Messaging Application

In order to use Communication Manager Messaging, you must verify with an account representative that the following Communication Manager features have been enabled in the license file:

- Maximum Administered IP Trunks - This number must be equal to or greater than the number of IP trunk ports used by Communication Manager Messaging.
- ARS
- ARS/AAR Partitioning
- ISDN-PRI
- H.323 Trunks (IP Trunks)
- Private Networking
- Uniform Dialing Plan
- Basic Call Setup
- Basic Supplementary Services
- Supplementary Services with Rerouting
- Transfer into QSIG Voice Mail
- Value-Added (VALU)

Inserting the Avaya S8300 Server (if necessary for standalone service or LSP)

The S8300 Server is inserted into the media gateway slot (For example, with G450, S8300B, S8300C, or S8300D can go into slot v1, or slot v5 whether it is the primary server or configured as a Local Survivable Processor (LSP).

Important:
The media gateway does not need to be powered down to insert or remove the S8300 server. The S8300 Server must be shutdown before removing it from the media gateway.

Terminal server installation

This section provides information on connecting adjunct equipment to a G700 or G350 Media Gateway with an S8300 Server using a terminal server (Figure 1: Switch-to-adjunct LAN connectivity through a terminal server). Avaya supports the IOLAN+ 104 terminal server.

Any device that does not support a direct TCP/IP connection, but that does support an RS232 interface, can connect through a terminal server. System printers and some CDR devices use RS232 connections and can connect through a terminal server.

You can connect up to four adjuncts through one terminal server.

Figure 1: Switch-to-adjunct LAN connectivity through a terminal server

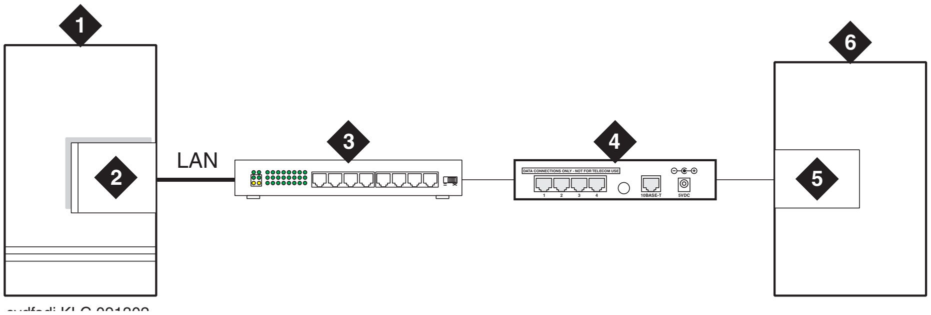


Figure notes:

1. **switch**
2. **IP connection on an S8300/G700 or G350 configuration**
3. **10/100Base-T Hub (optional)**
4. **terminal server**
5. **serial port**
6. **CDR adjunct**

Installing and administering the terminal server

Make sure you have all the equipment on site before the installation. You must have the hardware listed in Table 4: Required equipment.

Table 4: Required equipment

Comcode	Description	Qty	Supplier
700015084	IOLAN+ 104 communications server	1	Avaya
NA	RJ45-to-DB25 connector for IOLAN+ (supplied with 700015084)	4	Avaya
NA	DB25-to-DB9 connector for PC COM port	1	Avaya
NA	RS232 Null modem (if needed for PC or printer connectivity)	1 or more	Avaya
405369042	Male/female adapter (if necessary)	1 or more	Avaya
846943306 or 104154414 NA	6-inch RJ45 crossover cord, or 10/100Base-T auto-sensing LAN hub or router	1 1	Avaya Customer
102631413 NA	259A adapter, or CAT5 cross connect hardware and connecting blocks	1	Avaya Customer
NA	RJ45 UTP Category 5 modular cords	1–2	Customer
NA	451A in-line RJ45 adapters, as needed to connect modular cords together		

You also need a computer (laptop) with the HyperTerminal software program for the initial administration of the IOLAN+ and to set up the ports.

What are the distance limits for the terminal server

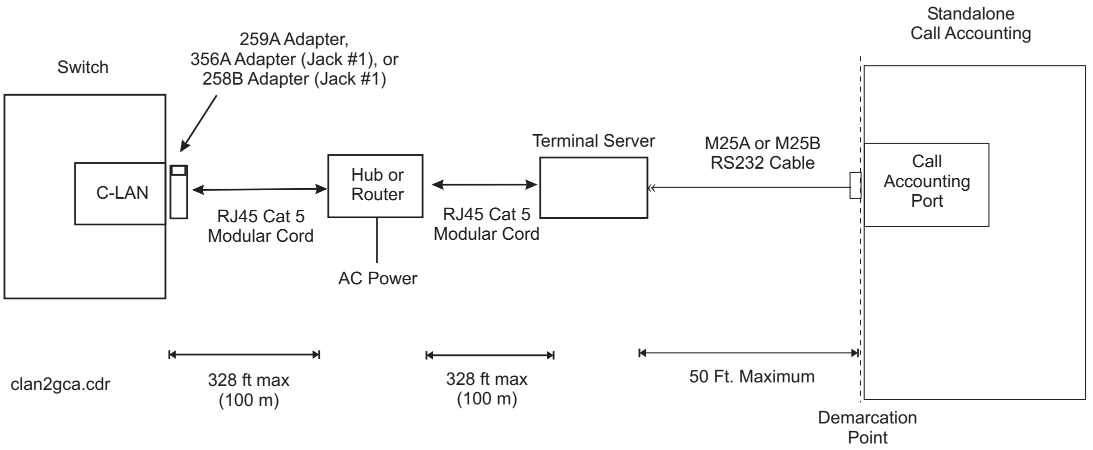
The distance limit from the switch to the LAN hub is 328 feet (100 meters). The distance limit from the LAN hub to the terminal server is 328 feet (100 meters). If installed, the limit from the terminal server to the adjunct is 50 feet (15 meters).

However, to achieve greater distance limits, the switch's LAN hub/router may be connected to a WAN and the hub/router for the terminal server also connected to the same WAN.

How is the terminal server cabling connected

Figure 2 shows the connection between the terminal server port and a call accounting system.

Figure 2: Stand-alone call accounting system link using a terminal server



Note:

> You can connect the S8300 Server directly to the terminal server with a data crossover cable. This connection eliminates the need for a hub or router in the middle, but the connection also allows the S8300 Server and the terminal server to communicate only with each other. With this connection, the S8300 Server and the terminal server should be configured with the same subnet.

The general connection process requires:

- Connecting the IOLAN+ to the adjunct and the LAN on page 62
- Administering the IOLAN+ on page 63
- Test the connectivity back through the switch

Connecting the IOLAN+ to the adjunct and the LAN

Connect the adjunct to the IOLAN+, using the RJ45-to-DB25 cable and the null modem. You can use a male/female adapter. See Figure 3: Connecting an adjunct to the IOLAN+ on page 63.

Figure 3: Connecting an adjunct to the IOLAN+

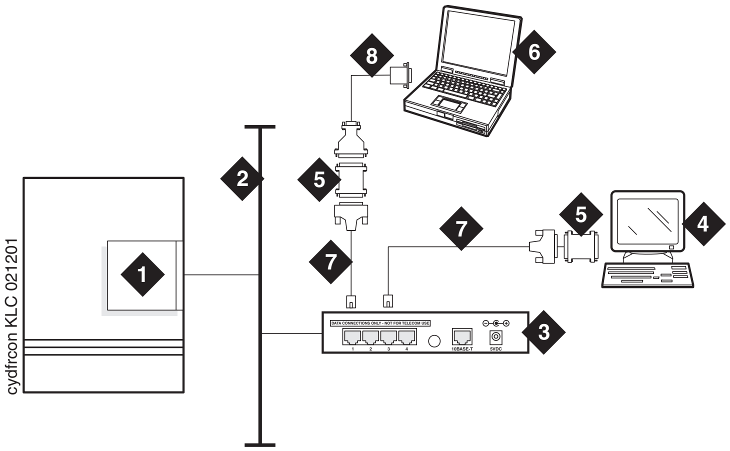


Figure notes:

1. **IP connection on an S8300/G700 or G350**
2. **Local area network (LAN)**
3. **IOLAN+ 104 terminal server**
4. **Adjunct (system management terminal or a system printer, for example)**
5. **Null modem**
6. **PC or laptop (for initial administration)**
7. **DB25-to-RJ45 cable**
8. **DB25-to-DB9 cable**

Note:

Depending on the adjunct's connections, you may not need all of these pieces.

To Connect the IOLAN+ to the adjunct and the LAN

1. Connect the null modem adapter to COM1 port on the adjunct.

Note:

The null modem is an important element in this setup. Without it, data may not transfer correctly.

2. Connect the other end of the null modem adapter to the DB25 to RJ45 cable.
3. Connect the RJ45 end to any port on the IOLAN+.

Administering the IOLAN+

To administer the IOLAN+ the first time, you must connect a PC or laptop to the RS232 Port 1 on the IOLAN+ terminal server. Follow these typical steps:

Note:

Depending on the computer's COM port, you may not need all of these pieces.

To connect the IOLAN+

1. Connect the DB9 end of the DB9-to-DB25 cable to the COM port on the PC or laptop.
2. Connect the DB25 end to the null modem adapter.
3. Connect the other end of the null modem adapter to the DB25 to RJ45 cable.
4. Connect the RJ45 end to Port 1 of the IOLAN+.

Before beginning the initial administration, make sure you have the following information:

- New IP address and subnet mask for IOLAN+
- Host name for IOLAN+
- IP address of S8300 Server Ethernet interface
- Port number of S8300 Server Ethernet interface where adjunct connects

Use the HyperTerminal software program that comes with Windows 95/98/NT/2000 to administer the IOLAN+.

To set up HyperTerminal on the computer

1. Open HyperTerminal.
2. Click **File > Properties > Connect** tab.

   In the Connect using: field, select **COM *n***

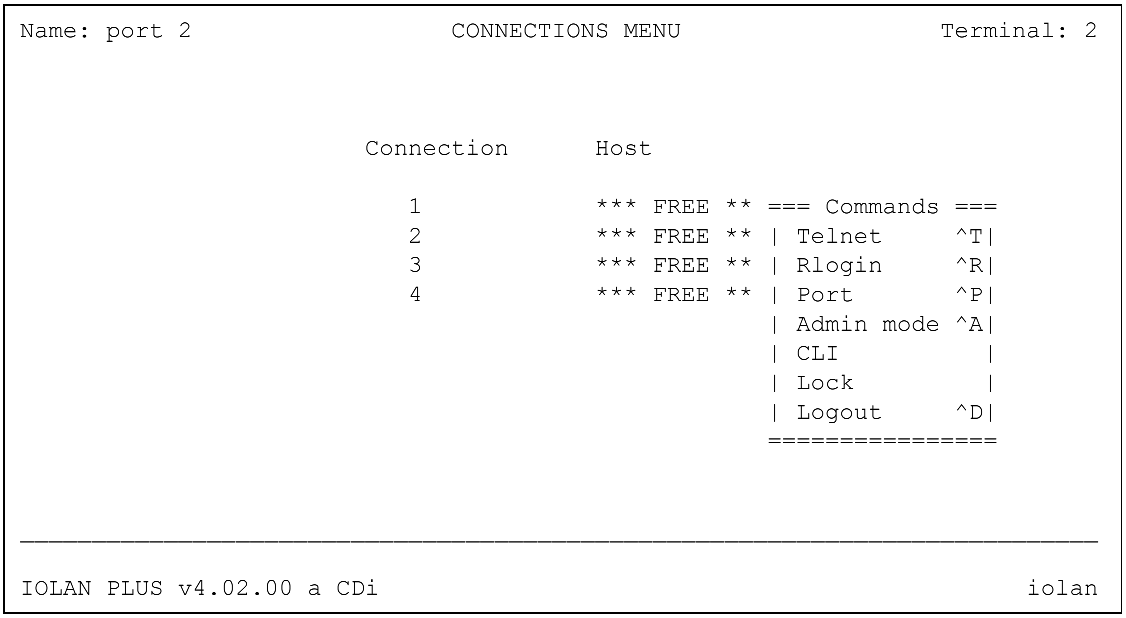
   where ***n*** is the communication port your computer is using.
3. Click **CONFIGURE**

   Set the **bits per second** field to **9600**.

   Set the **Flow control** field to **Hardware**.
4. Click **OK**.
5. Press **ENTER** to get the login prompt.

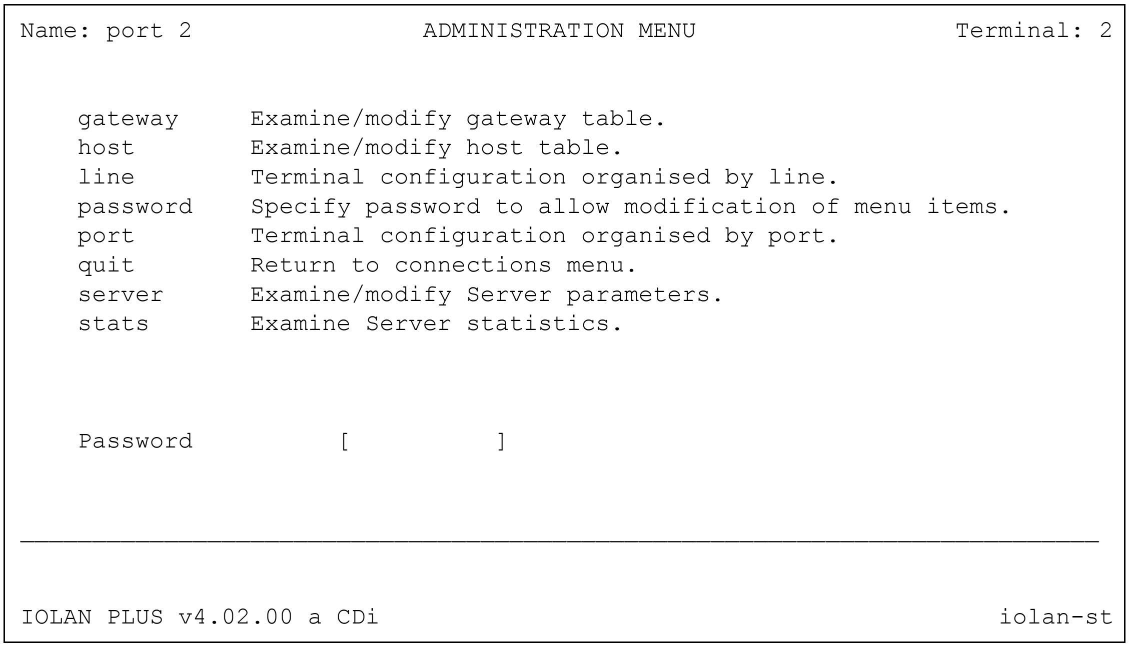
To administer the IOLAN+ the first time

1. At the login prompt type **any text** and press **ENTER**.
2. At the second prompt type **`set term ansi`** and press **ENTER** to view the **Connections Menu**.



```
Name: port 2                  CONNECTIONS MENU                 Terminal: 2



                        Connection      Host

                           1            *** FREE ** === Commands ===
                           2            *** FREE ** | Telnet     ^T|
                           3            *** FREE ** | Rlogin     ^R|
                           4            *** FREE ** | Port       ^P|
                                                    | Admin mode ^A|
                                                    | CLI          |
                                                    | Lock         |
                                                    | Logout     ^D|
                                                    ================


___________________________________________________________________________

IOLAN PLUS v4.02.00 a CDi                                            iolan
```

3. Under **Connection** select **Port 1** (the port to which the adjunct is connected) and press **ENTER** to access the **Commands** menu.
4. Select **Admin mode > Password** and press **ENTER**.

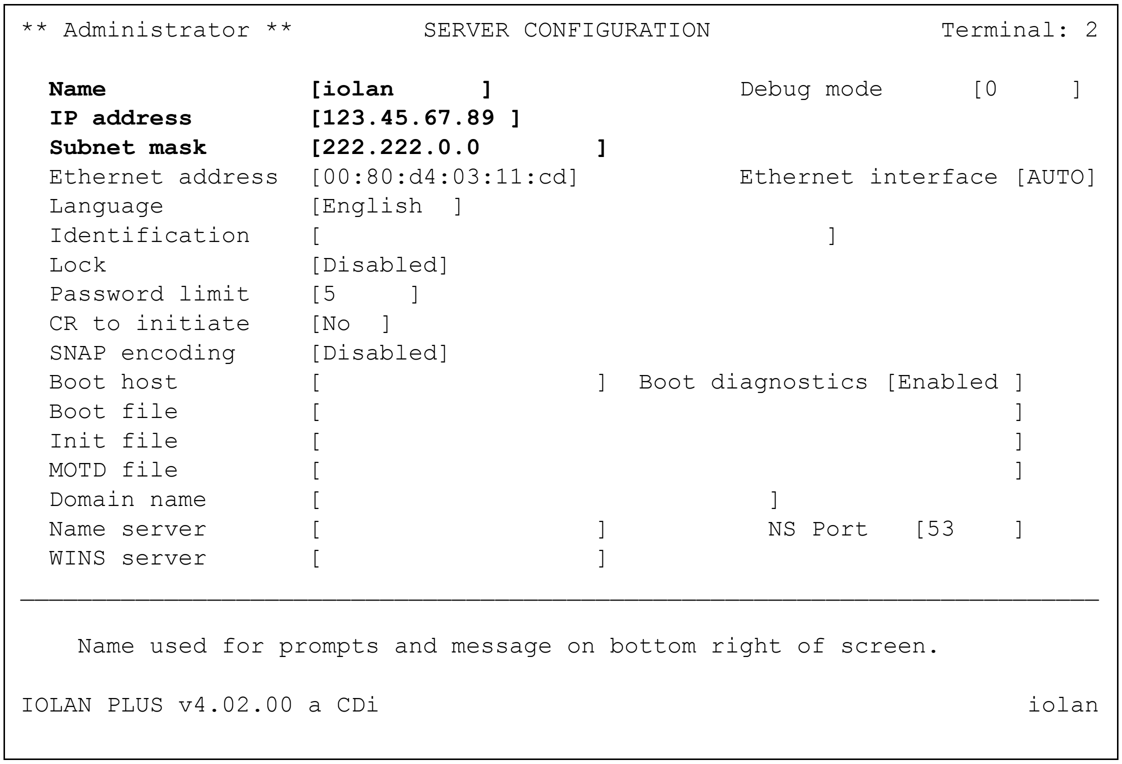


```
Name: port 2                ADMINISTRATION MENU                 Terminal: 2


    gateway     Examine/modify gateway table.
    host        Examine/modify host table.
    line        Terminal configuration organised by line.
    password    Specify password to allow modification of menu items.
    port        Terminal configuration organised by port.
    quit        Return to connections menu.
    server      Examine/modify Server parameters.
    stats       Examine Server statistics.



    Password          [          ]



___________________________________________________________________________


IOLAN PLUS v4.02.00 a CDi                                          iolan-st
```

5. Type **iolan**, the default password, and press **ENTER**.

   The **Administration Menu** changes, offering more options.

6. Select **server** and press **ENTER** to view the **Server Configuration** menu.



```
** Administrator **         SERVER CONFIGURATION                Terminal: 2

  Name              [iolan      ]                 Debug mode      [0     ]
  IP address        [123.45.67.89 ]
  Subnet mask       [222.222.0.0        ]
  Ethernet address  [00:80:d4:03:11:cd]           Ethernet interface [AUTO]
  Language          [English  ]
  Identification    [                                    ]
  Lock              [Disabled]
  Password limit    [5     ]
  CR to initiate    [No  ]
  SNAP encoding     [Disabled]
  Boot host         [                   ]  Boot diagnostics [Enabled ]
  Boot file         [                                                ]
  Init file         [                                                ]
  MOTD file         [                                                ]
  Domain name       [                                ]
  Name server       [                   ]           NS Port   [53    ]
  WINS server       [                   ]
___________________________________________________________________________

    Name used for prompts and message on bottom right of screen.

IOLAN PLUS v4.02.00 a CDi                                             iolan
```

7. Fill in the following fields with information appropriate to your network.

   Leave the default settings for the other fields.

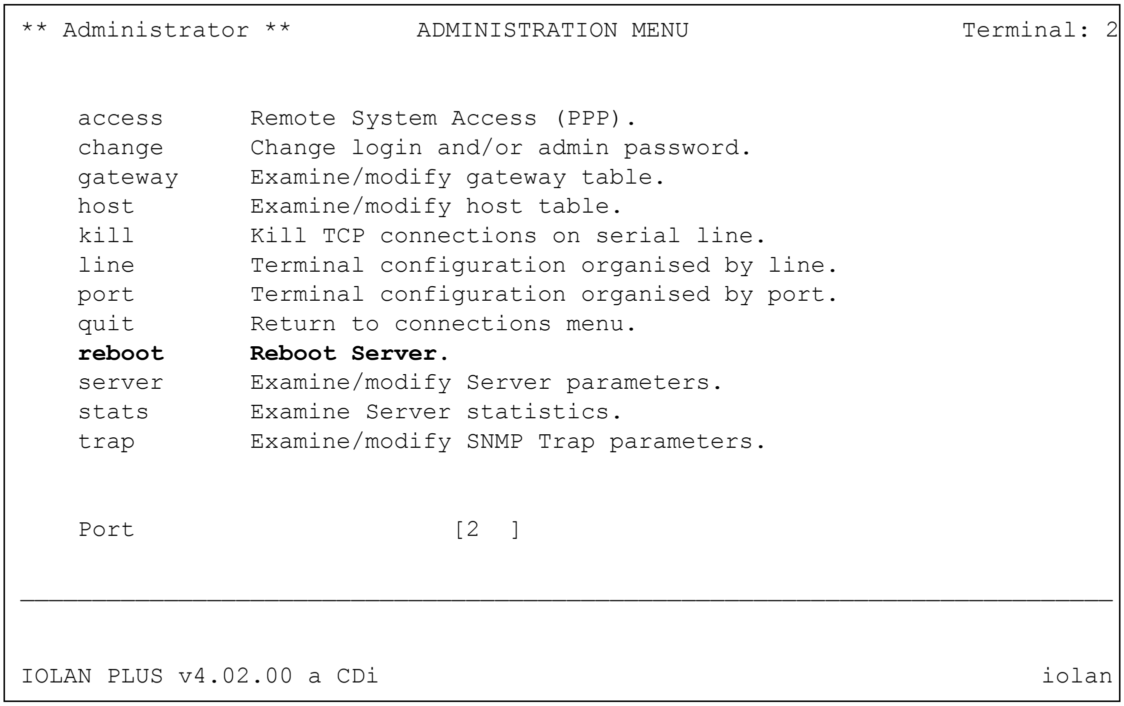
   - **Name:**
   - **IP address:** (for IOLAN+)
   - **Subnet mask:**

8. Press **ENTER** and select **Save & Exit** to effect the changes.

You must reboot the server any time you change an **IP address** or **Local Port** value.

To reboot the IOLAN+

1. Press **ENTER** to view the **Administration Menu**.



```
** Administrator **        ADMINISTRATION MENU                 Terminal: 2


    access      Remote System Access (PPP).
    change      Change login and/or admin password.
    gateway     Examine/modify gateway table.
    host        Examine/modify host table.
    kill        Kill TCP connections on serial line.
    line        Terminal configuration organised by line.
    port        Terminal configuration organised by port.
    quit        Return to connections menu.
    reboot      Reboot Server.
    server      Examine/modify Server parameters.
    stats       Examine Server statistics.
    trap        Examine/modify SNMP Trap parameters.


    Port                      [2  ]

____________________________________________________________________________


IOLAN PLUS v4.02.00 a CDi                                              iolan
```

Note:

The following steps re-initialize the IOLAN+ so it knows it's connected to the LAN through its IP address.

2. Select **reboot** and press **ENTER**.
3. Press the space bar to restart the IOLAN+.

Navigating the IOLAN+ terminal server

Refer to the IOLAN+ user guide for details. In general, you must:

- Use the arrow keys to move to a menu item.
- Use the **TAB** key to move from field to field horizontally.
- Use the **ENTER** key to choose an item.

Administering the gateway

Note:

If the S8300 Server and IOLAN+ are in the same subnet, skip this step.

To administer the gateway for IOLAN+

1. Select **Admin mode > Password** and press **ENTER**.
2. Type **iolan** and press **ENTER**.
3. Select **gateway** to access the **Gateway** menu.
4. Fill in the following fields for **Entry 1**:
   - **Destination:** S8300 Server *IP address*
   - **Gateway:** *Gateway address*
   - **Netmask:** *Subnet mask*

   Note:

   The following steps re-initialize the IOLAN+ so it knows it's connected to the LAN through your gateway.
5. Select **reboot** and press **ENTER**.
6. Press the space bar to restart the IOLAN+.

Administering an IOLAN+ port

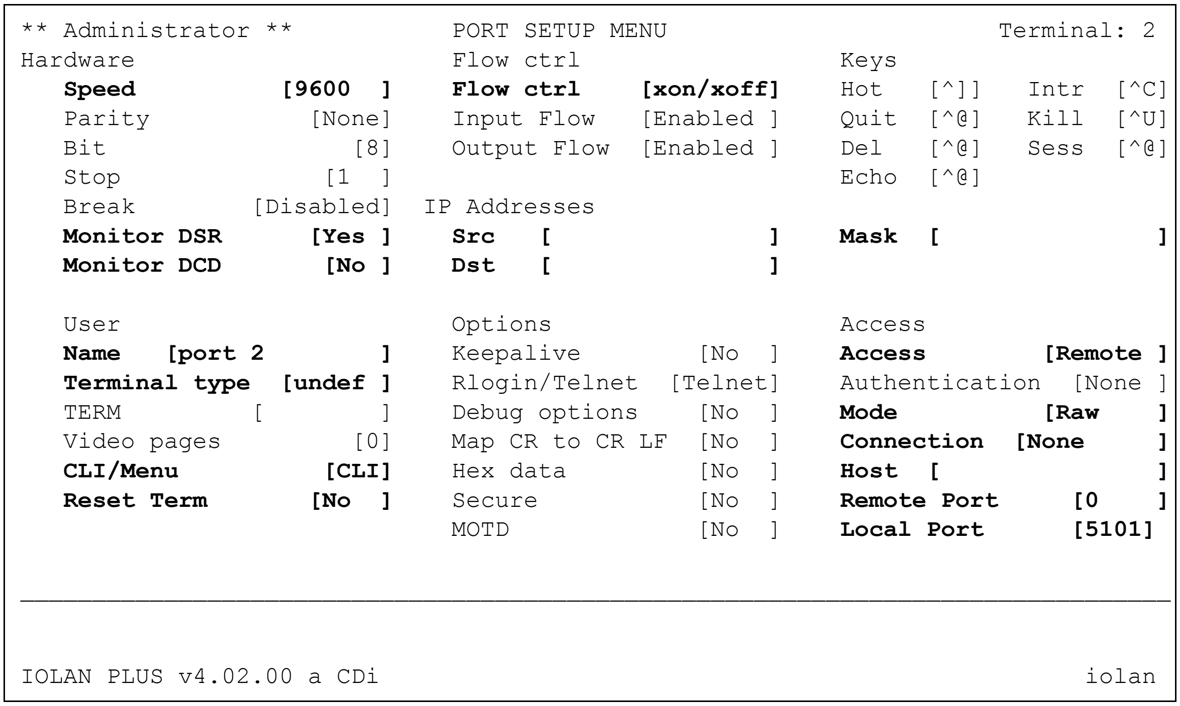
Use this procedure when connecting an adjunct or serial COM port on a PC directly (locally) to the IOLAN+ (see Figure 3: Connecting an adjunct to the IOLAN+ on page 63).

To administer an IOLAN+ port

1. Select **Admin mode > Password** and press **ENTER**.
2. Type **iolan** and press **ENTER**.
3. Select **port** and press **ENTER**.

4. Type ***port number*** and press **ENTER** to view the **Port Setup Menu**

   where ***port number*** is the port that the adjunct connects to,



```
** Administrator **           PORT SETUP MENU                       Terminal: 2
Hardware                      Flow ctrl                  Keys
   Speed          [9600  ]    Flow ctrl    [xon/xoff]    Hot   [^]]   Intr  [^C]
   Parity           [None]    Input Flow   [Enabled ]    Quit  [^@]   Kill  [^U]
   Bit                 [8]    Output Flow  [Enabled ]    Del   [^@]   Sess  [^@]
   Stop               [1  ]                              Echo  [^@]
   Break        [Disabled]  IP Addresses
   Monitor DSR      [Yes ]    Src    [               ]   Mask  [               ]
   Monitor DCD       [No ]    Dst    [               ]

   User                       Options                    Access
   Name   [port 2        ]    Keepalive        [No  ]    Access        [Remote ]
   Terminal type  [undef ]    Rlogin/Telnet  [Telnet]    Authentication  [None ]
   TERM         [        ]    Debug options    [No  ]    Mode          [Raw    ]
   Video pages         [0]    Map CR to CR LF  [No  ]    Connection  [None     ]
   CLI/Menu          [CLI]    Hex data         [No  ]    Host  [               ]
   Reset Term       [No  ]    Secure           [No  ]    Remote Port     [0    ]
                              MOTD             [No  ]    Local Port      [5101]

________________________________________________________________________________


IOLAN PLUS v4.02.00 a CDi                                                 iolan
```

5. Fill in the following fields.

   Leave the default settings for the other fields.

   - **Speed: 9600**
   - **Monitor DSR: Yes**
   - **Monitor DCD: No**
   - **Name:** *port number or other descriptive name*
   - **Terminal type: undef**
   - **CLI/Menu: CLI**
   - **Reset Term: No**
   - **Flow ctrl: xon/xoff**
   - **IP addresses:** *leave blank*
   - **Mask:** *leave blank*
   - **Access: Remote**
   - **Authentication: None**
   - **Mode: Raw**
   - **Connection: None**

- **Host:** *leave blank or enter S8300 Server IP Address*
- **Remote Port:** *0*
- **Local Port:** *must match the value of Remote Port on the IP Services screen of the Communication Manager software*

6. Press **ENTER** and select **Save & Exit** to effect the changes.
7. Press **ENTER** again to view the **Administration Menu**.
8. Select **kill** to disable the port connection.
9. Repeat the steps for each additional port you want to administer.
10. When administration is complete, from the **Connections Menu**, select **logout** (or press **Ctrl D**).
11. Close HyperTerminal.

At this point, you have established a connection path from the adjunct through the IOLAN+ to the S8300 Server.

Testing connectivity through the IOLAN+

To test connectivity through the IOLAN+

1. On the system management terminal, press **ENTER** to get the login prompt to the Communication Manager switch.

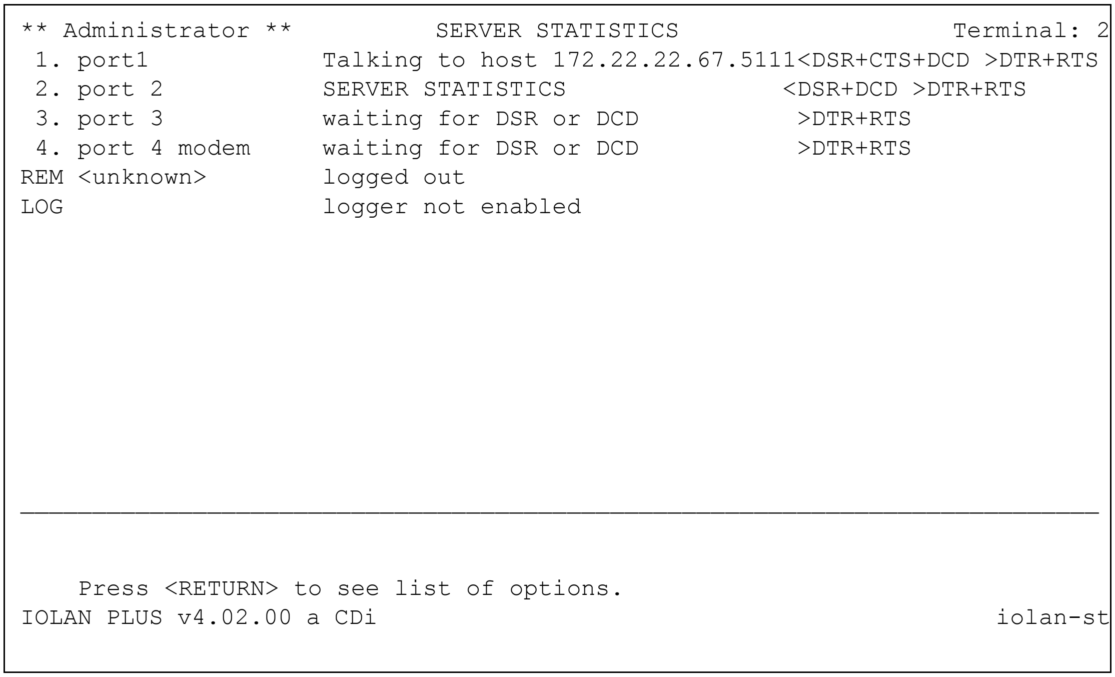
   Note:

   If you get garbled text, check the baud rate setting on the **Port Setup Menu**. You can adjust it up or down.

2. If no login prompt appears, log back into the IOLAN+ through HyperTerminal.
3. Select **Admin mode > stats** and press **ENTER** twice.
4. Select **users** and press **ENTER**.

5. Look at the port that the adjunct is connected to and see if there is any traffic.

   If not, check all your connections and administration fields.

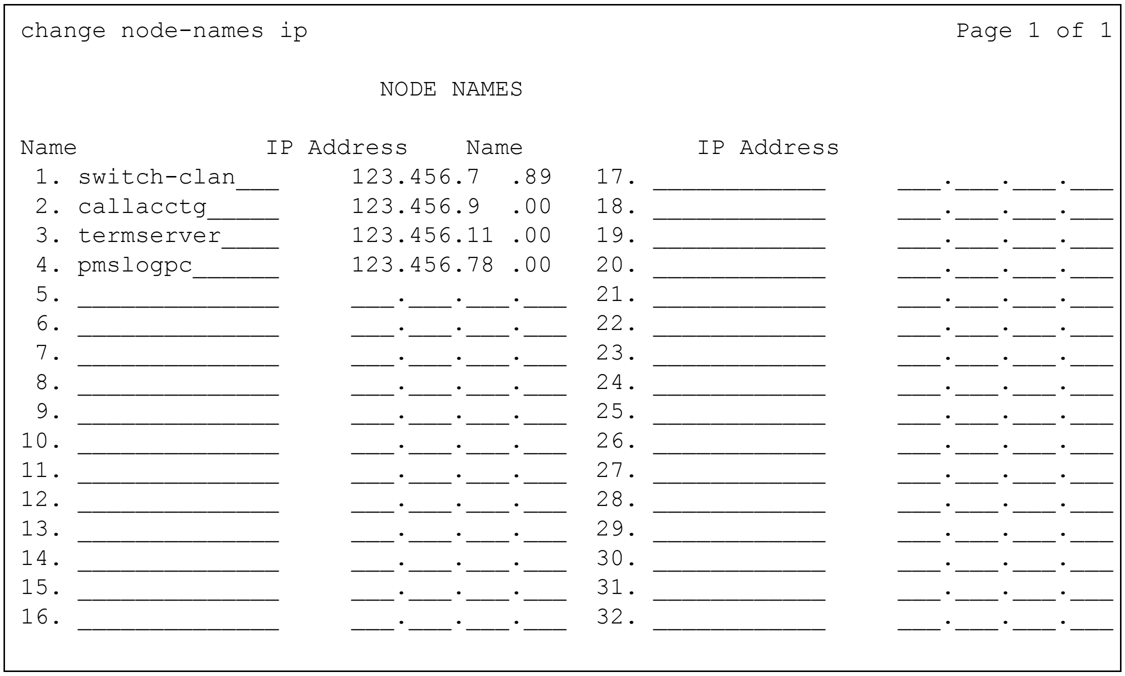


```
** Administrator **          SERVER STATISTICS                   Terminal: 2
 1. port1            Talking to host 172.22.22.67.5111<DSR+CTS+DCD >DTR+RTS
 2. port 2           SERVER STATISTICS              <DSR+DCD >DTR+RTS
 3. port 3           waiting for DSR or DCD          >DTR+RTS
 4. port 4 modem     waiting for DSR or DCD          >DTR+RTS
REM <unknown>        logged out
LOG                  logger not enabled










____________________________________________________________________________



    Press <RETURN> to see list of options.
IOLAN PLUS v4.02.00 a CDi                                               iolan-st
```

After you have successfully administered and validated the connection between the adjunct and the S8300 Server through the IOLAN+, you can disconnect the laptop or other PC from the IOLAN+. No further IOLAN+ administration is required.

Potential failure scenarios and repair actions

If a link goes down between the terminal server and the switch, you must reboot the terminal server for the link come back up. If you are performing a software upgrade or if a system reset occurs, you must reboot the terminal server to restore the link. See To reboot the IOLAN+ on page 67.



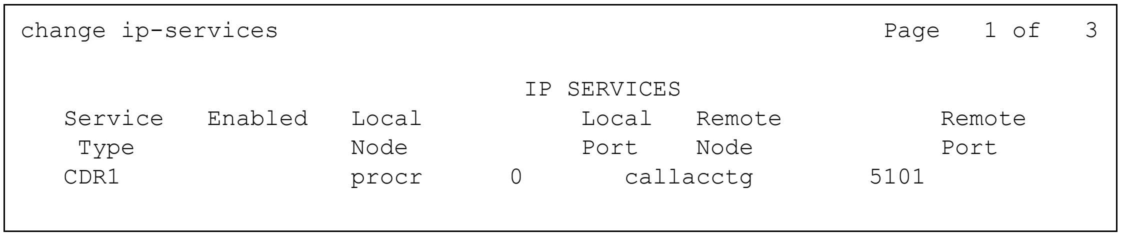
```
change node-names ip                                              Page 1 of 1

                         NODE NAMES

Name             IP Address    Name             IP Address
 1. switch-clan___     123.456.7  .89   17. ____________     ___.___.___.___
 2. callacctg_____     123.456.9  .00   18. ____________     ___.___.___.___
 3. termserver____     123.456.11 .00   19. ____________     ___.___.___.___
 4. pmslogpc______     123.456.78 .00   20. ____________     ___.___.___.___
 5. ______________     ___.___.___.___  21. ____________     ___.___.___.___
 6. ______________     ___.___.___.___  22. ____________     ___.___.___.___
 7. ______________     ___.___.___.___  23. ____________     ___.___.___.___
 8. ______________     ___.___.___.___  24. ____________     ___.___.___.___
 9. ______________     ___.___.___.___  25. ____________     ___.___.___.___
10. ______________     ___.___.___.___  26. ____________     ___.___.___.___
11. ______________     ___.___.___.___  27. ____________     ___.___.___.___
12. ______________     ___.___.___.___  28. ____________     ___.___.___.___
13. ______________     ___.___.___.___  29. ____________     ___.___.___.___
14. ______________     ___.___.___.___  30. ____________     ___.___.___.___
15. ______________     ___.___.___.___  31. ____________     ___.___.___.___
16. ______________     ___.___.___.___  32. ____________     ___.___.___.___
```

Administering IP services

For each adjunct that you connect using TCP/IP, you need to administer IP services to establish the IP address/TCP port pairing. The IP address is associated with the node name that you just administered. In this example, we are administering the primary call detail recording (CDR) connection as end-to-end TCP/IP.

To administer IP services

1. Type **change ip-services** and press **RETURN** to assign the CDR endpoint.
2. In the `Service Type` field, enter **CDR1** for the call accounting link.



```
change ip-services                                          Page   1 of   3

                                   IP SERVICES
   Service   Enabled   Local           Local   Remote           Remote
    Type               Node            Port    Node             Port
   CDR1                procr      0       callacctg        5101
```

3. In the **Local Node** field, enter the node name for the switch.

   In this example, enter **procr**.
4. The **Local Port** field defaults to `0` for all client applications.

   You cannot make an entry in this field.
5. In the **Remote Node** field, enter the node name for the adjunct, as administered on the **Node Names** screen.

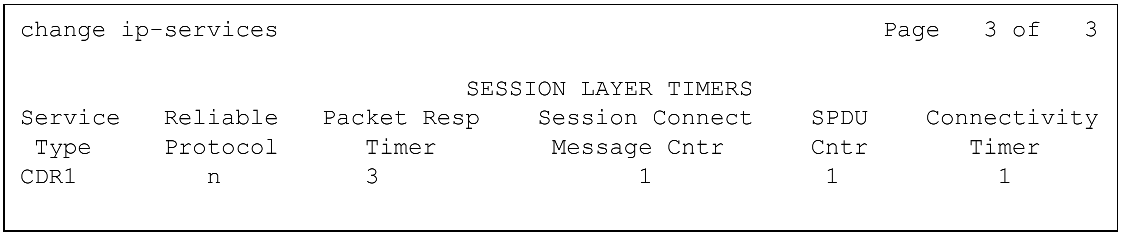
   For the call accounting application, type **callacctg**.
6. In the **Remote Port** field, enter the TCP listen port assigned to the adjunct.

   The recommended value for CDR1 is 5101.

   Note:

   > This number must match the port administered on the end device. If you are using the Downloadable Reliable Session-Layer Protocol tool, this must match the port administered in the Server application. If you are using a terminal server, this number must match the `Local Port` number on the Port Setup menu. Consult the documentation for your Call Accounting system to determine the appropriate port for the CDR device.
7. Go to Page 3 and type **n** in the **Reliable Protocol** field for the CDR Service Type.

   You do not use RSP with a terminal server.



```
change ip-services                                          Page   3 of   3

                               SESSION LAYER TIMERS
Service   Reliable   Packet Resp    Session Connect    SPDU    Connectivity
 Type     Protocol      Timer        Message Cntr      Cntr       Timer
CDR1         n          3                  1            1           1
```

8. Press **ENTER** to save your changes.

Call detail recording (CDR)

This section provides information on connecting call detail recording (CDR) equipment.

Connecting CDR equipment

The interface between an Avaya Server and CDR equipment is a Processor Ethernet Connection.

CDR equipment connects to one of the two IP connections (EXT 1 or EXT 2) on the front of the G700 or G350 Media Gateway. As with C-LAN connections, the CDR adjunct may be a terminal server or a CDR application using RSP.

Note:

A printer or customer premises equipment (CPE) can also be used as the output receiving device. Please see Printers on page 79 of this book for instructions on using a printer.

Administering CDR data collection

Note:

To send CDR data using a processor Ethernet interface to a device on the LAN/ WAN, you have the option to enable/disable RSP.

To administer CDR Data Collection

1. Setup the CDR adjunct to be ready to collect CDR data.

   Record the **IP address** and the **port number** of the CDR adjunct, which could be a terminal server or a CDR application that uses RSP.

   If the CDR adjunct is an application that uses RSP, start the application to listen for a client connection at the port.

2. Access the **IP Services** screen in Communication Manager (see Administering IP services on page 72), and do the following:

   a. In the **Service Type** field, enter **CDR1** or **CDR2**.

   b. In the **Local Node** field, enter **procr**.

   c. The **Local Port** field defaults to `0` for all client applications.

      You cannot make an entry in this field.

   d. In the **Remote Node** field, enter the node name you assigned to the CDR adjunct in step 2.

   e. In the **Remote Port** field, enter the port number used by the CDR adjunct determined in step 1.

3. Go to Page 3 and do the following:

   a. Enter **y** in the **Reliable Protocol** field if you have a CDR application using RSP.

      Enter **n** if the CDR adjunct is connected through a terminal server.

   b. If RSP is being used, complete the **Packet Resp Timer** and **Connectivity Timer** fields with a reasonable value that matches the network condition (recommended values are **30** and **60** seconds, respectively).

   c. Accept the defaults in the other fields.

4. Administer CDR parameters as described in Administering CDR parameters on page 75.

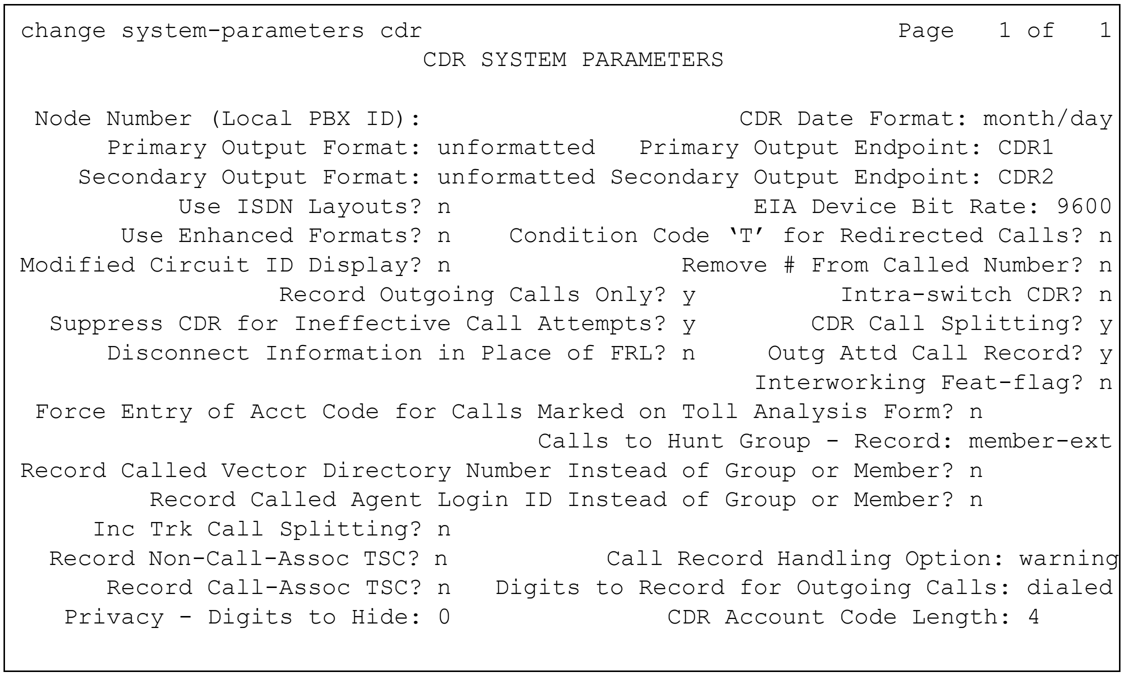
Administering CDR parameters

You must administer CDR parameters to let the system know that the adjunct is connected through TCP/IP. For details on all fields on the **CDR System Parameters** screen, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

To administer CDR parameters

1. Type **change system-parameters cdr** and press **RETURN**.

   The **CDR System Parameters** screen appears.



```
change system-parameters cdr                                 Page   1 of   1
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID):                      CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
           Use ISDN Layouts? n                     EIA Device Bit Rate: 9600
       Use Enhanced Formats? n    Condition Code ‘T’ for Redirected Calls? n
Modified Circuit ID Display? n                Remove # From Called Number? n
                  Record Outgoing Calls Only? y          Intra-switch CDR? n
  Suppress CDR for Ineffective Call Attempts? y        CDR Call Splitting? y
      Disconnect Information in Place of FRL? n     Outg Attd Call Record? y
                                                   Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
         Record Called Agent Login ID Instead of Group or Member? n
     Inc Trk Call Splitting? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 4
```

2. In the **Primary Output Format** field, enter a format specific to the call accounting system, if necessary.

   In the example, **unformatted** is used. If you were sending data directly to a printer, you would use **printer**.

3. In the **Primary Output Endpoint** field, type **CDR1**.

4. If you use a secondary output device, and that device is also connected through TCP/IP, complete the **Secondary Output Format** field.

   Also, type **CDR2** in the **Secondary Output Endpoint** field.

5. Press **ENTER** to save your changes.

Testing the switch-to-adjunct link

You can use the test, status, busyout and release commands to find and correct problems with CDR links. For more information about these commands, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

```
status cdr-link
                              CDR LINK STATUS
                Primary                          Secondary

       Link State: up                            extension not administered

 Maintenance Busy? no
```

Work with the vendor to test the link from the call accounting adjunct.

If a link does not come up immediately, use the **busyout cdr-link** and **release cdr-link** commands to bring up the link.

Additional administration procedures for CDR equipment are provided in the *Administering Avaya Aura™ Communication Manager*, 03-300509.

Reliable Data Transport Tool (RDTT) package

Avaya provides this free software application to help vendors and customers develop CDR applications that use the reliable session protocol to collect CDR data from an Avaya server. The Reliable Data Transport Tool (RDTT) is a testing tool and thus is not supported by Avaya.

What does the RDTT package contain

The RDTT package consists of the following:

- Specifications for the Reliable Session Protocol
- The Client application (Client.exe)

  This application is designed to help you test the reliable session protocol without use of an Avaya server.
- The Server application (Server.exe)

  This application is designed to help you understand the reliable session protocol and to start building your products to work with the Avaya Server.

- User Guide

  This document contains information about the client and server applications.

Downloading the RDTT package

The RDTT package is available from the Avaya support Web site as a self-extracting executable.

To download the RDTT package

1. Go to the Avaya Customer Support Web site at http://avaya.com/support.
2. In the **Search For** text box, type **reliable** and click **Go**.
3. Select **Reliable Data Transport Client/Server Tool** from the list of links that are found.
4. When asked, save the **RDTT.exe** file to a temporary folder on your computer.

   It is approximately 1.6 to 2.0MB in size.

Installing the RDTT package

To install the RDTT package

1. Double-click the **RDTT.exe** file.

   The Install Shield Wizard steps you through the installation.
2. When prompted to select Client or Server, select both programs.
3. Continue with the installation.

   Use the default destination folder and program folder.

Administering the RDTT package

See the instructions in the user_guide.doc file to administer the RDTT tool on a PC.

Related topics

See the following topics related to CDR:

- Chapter 16, “Collecting Billing Information,” in *Administering Avaya Aura™ Communication Manager*, 03-300509.

- “Call Detail Recording” in Chapter 21, “Features and Technical Reference” in *Administering Avaya Aura™ Communication Manager*, 03-300509.

Printers

For connecting a printer to a G700 or G350 Media Gateway, see Terminal server installation on page 60 for more information.

DS1/T1 CPE loopback jack

This section provides information on how to install and use a DS1 loopback jack to test the DS1 span between the Avaya server or gateway and the network interface point. *The loopback jack is required when DC power is at the interface to the integrated channel service unit (ICSU)*.

Note:

Do not remove the loopback jack after installation. It should always be available for remote tests of the DS1 span.

Note:

Note:

For G700 or G350 Media Gateway systems, the channel service unit (CSU) is integrated within the MM710 Media Module. This means that there is no need for a separate external device. The loopback jack isolates the MM710 internal CSU from the DC power and properly loops the DC span power.

This section covers:

- Installing a loopback jack on page 80
- Administering a loopback jack on page 82
- Testing a loopback jack with a smart jack on page 82
- Testing a loopback jack without a smart jack on page 91
- Configurations using fiber multiplexers on page 94

Installing a loopback jack

You can use one of two installation options:

- Installing a loopback jack with a smart jack on page 80
- Installing a loopback jack without a smart jack on page 81

Installing a loopback jack with a smart jack

Use one of the following installation methods:

- Install the loopback jack at the interface to the smart jack, if possible.

  This position provides maximum coverage of CPE wiring when remote loopback tests are run.

- If the smart jack is not accessible, install the loopback jack at the extended demarcation point.

- If there is no extended demarcation point, install the loopback jack directly at the network interface point as shown in Figure 4: Network interface at smart jack for an MM710 multi-media module on page 88.
- If there is an extended demarcation point and the smart jack is not accessible, install the loopback jack as shown in Figure 5: Network interface at extended demarcation point (smart jack inaccessible) for an MM710 multi-media module on page 89.
- If there is an extended demarcation point, but the smart jack is accessible, install the loopback jack as shown in Figure 6: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module on page 90.

To install the loopback jack with a smart jack

1. Disconnect the RJ-48 (8-wide) connector at the appropriate interface point, and connect the loopback jack in series with the DS1 span.

   See Figure 4: Network interface at smart jack for an MM710 multi-media module on page 88 through Figure 6: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module on page 90.
2. Plug the H600-383 cable from the MM710 into the female connector on the loopback jack.
3. Plug the male connector on the loopback jack cable into the network interface point.

   Note:

   Do not remove the loopback jack after installation. This is not a test tool and should always be available to remotely test a DS1 span.

Installing a loopback jack without a smart jack

Use one of the following installation methods:

- Install the loopback jack at the point where the cabling from the ICSU plugs into the *dumb* block.
- If there is more than one *dumb* block, choose the one that is closest to the Interface Termination feed or the fiber MUX, to provide maximum coverage for loopback jack tests.

  Refer to Figure 7: Network interface at “dumb” block for an MM710 multi-media module on page 91 and Figure 8: Network interface at “dumb” block with repeater line to fiber MUX for an MM710 multi-media module on page 92.

To install the loopback jack without a smart jack

1. Disconnect the RJ-48 (8-wide) connector at the appropriate interface point, and connect the loopback jack in series with the DS1 span.

   See Figure 7: Network interface at “dumb” block for an MM710 multi-media module on page 91 through Figure 8: Network interface at “dumb” block with repeater line to fiber MUX for an MM710 multi-media module on page 92.

2. Plug the H600-383 cable from the ICSU, or from the MM710, into the female connector on the loopback jack.
3. Plug the male connector on the loopback jack cable into the network interface point.

   Note:

   Do not remove the loopback jack after installation. This is not a test tool and should always be available to remotely test a DS1 span.

Administering a loopback jack

To administer a loopback jack

1. At the management terminal, type `change ds1 location`

   where ***location*** is the DS1 interface circuit pack corresponding to the loopback jack.
2. Verify that the **near-end CSU** type is set to `integrated`.
3. On page 2 of the form, change the **supply CPE loopback jack power** field to `y`.

   Setting this field to `y` informs the technician that a loopback jack is present on the facility and allows the technician to determine that the facility is available for remote testing.
4. Enter `save translation` to save the new information.

Testing a loopback jack with a smart jack

The loopback jack and smart jack isolate faults by dividing the DS1 span into three sections (see Figure 4: Network interface at smart jack for an MM710 multi-media module on page 88 through Figure 6: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module on page 90).

These three sections are:

- From the MM710 to the loopback jack
- From the loopback jack to the smart jack (network interface point)
- From the smart jack to the CO

The first two sections are your responsibility. The last is the responsibility of the DS1 service provider.

Testing the DS1 span from the ICSU to the loopback jack

The DS1 span test has 2 parts:

- Checking for circuit connectivity. The first part of the test powers-up the loopback jack and sends a signal from the DS1 circuit pack, through the wiring, to the loopback jack. The test allows about 10 seconds for the signal to loop around the loopback jack and return to the DS1 circuit pack. Then it sends the results to the management terminal and proceeds to the second part of the test.
- The second part of the test sends the standard, 3-in-24 DS1 stress-testing pattern from the DS1 board, through the loopback jack, and back to a bit error detector and counter on the DS1 board. A bit-error rate counter displays the results on the management terminal until you terminate the test.

Always perform both parts of the test. Proceed as follows.

Checking the integrity of local equipment

Before you go any further, make sure that the problem is actually on the DS1 span by testing the equipment that connects to the span at the near end. Test the DS1 circuit pack, and perform any needed maintenance or repairs.

To test the DS1 span

1. On the SAT, type **`busyout board`** ***XXXVS***

   where ***XXX*** is the administered number of the G700 or G350 (for example, **002**), and ***VS*** is the slot number on the G700 or G350 of the Media Module (for example, **V3**). The ***V*** is not a variable and needs to be included in the command exactly where shown. A sample address for a DS1 circuit pack on a G700 or G350 Media Gateway might look like this: **002V3**.

2. Type **`busyout board`** ***XXXVS***

   where ***XXX*** is the administered number of the G700 or G350 (for example, 002), and ***VS*** is the slot number on the G700 or G350 of the Media Module (for example, V3).

3. Type **`change ds1`** ***XXXVS*** to open the **DS1 administration** form.

4. Make sure that the **near-end csu type** field is set to `integrated`.

5. Go to page 2 of the **DS1 administration** form, and verify that the value of the **TX LBO** field is `0dB`.

6. If the value of the **TX LBO** field is not `0dB`, record the current value.

   Then set the **TX LBO** field to `0dB` for testing.

7. Press **ENTER** to make the changes.

8. Type **`test ds1-loop`** ***XXXVS*** **`cpe-loopback-jack`**

   where ***XXX*** is the administered number of the G700 or G350 (for example, 002), and ***VS*** is the slot number on the G700 or G350 of the Media Module (for example, V3).

   The loopback jack powers up. Active, DS1 facility alarms (if any) clear. After about 20 seconds, the first set of results appears on the terminal.

9. If `FAIL` appears on the terminal display, there may be a fault in the wiring between the ICSU and the loopback jack or the loopback jack may itself be faulty.

   Isolate the problem by replacing the loopback jack and repeating Step 8.

10. If `FAIL` still appears after the loopback jack has been replaced, suspect a wiring problem.

    Replace the cable between the ICSU and the loopback jack. Then repeat Step 8.

11. When `PASS` appears on the terminal, proceed with the second part of the test, checking the integrity of transmitted data.

Testing the integrity of data sent over the loop

Now perform the second part of the test, checking for data errors.

Note:

The loss of signal (LOS) alarm (demand test #138) is not processed during this test while the 3-in-24 pattern is active.

To test the integrity of data sent over the loop

1. At the SAT, type **`clear meas ds1 loop`** ***XXXVS*** to zero out the bit-error counter.

   where ***XXX*** is the administered number of the G700 or G350 (for example, **002**), and ***VS*** is the slot number on the G700 or G350 of the Media Module (for example, **V3**).

2. Type **`clear meas ds1 log`** ***XXXVS*** to zero out the performance measurement counter.
3. Type **`clear meas ds1 esf`** XXXVS to zero out the ESF error count.
4. Type **`list meas ds1 sum`** ***XXXVS*** to display the bit error count.
5. Step through Table 5: DS1 Troubleshooting to troubleshoot.

Table 5: DS1 Troubleshooting

Condition	Solution
The value of the **Test: cpe-loopback-jack** field is `Pattern 3-in-24`	The loopback jack test is active.
The value of the **Synchronized** field is `N`	Retry the test 5 times.
The value of the **Synchronized** field remains `N` after 5 tries	Excessive bit errors are likely. Check for intermittent connections or broken wires in an SPE receive or transmit pair, and repair as necessary. Then repeat Step 1.
The value of the **Bit-error count** field is *non-zero*	Repeat Step 1 several times.

1 of 2

Table 5: DS1 Troubleshooting (continued)

Condition	Solution
The value of the **Synchronized** field is `Y`	The DS1 circuit pack has synchronized to the looped 3-in-24 pattern and is counting bit errors in the pattern.
The value of the **Bit-error count** field pegs at `75535` or increments by 100s or 1000s each time you repeat Step 1	Suspect loose or corroded connections, severe crosstalk, or impedance imbalances between the two conductors of the receive or transmit pair. Wiring may need replacement.
The value of the **Bit-error count** field is `0`	There are no obvious wiring problems. Verify this by repeating Step 1 at 1-minute to 10-minute intervals until you are certain. If the test reports no errors for 1 minute, the error rate is less than 1 in 10^8. If the test reports no errors for 10 minutes, the error rate is less than 1 in 10^9.
	2 of 2

Once you are fairly certain that the test is reporting no errors (after at least 1 error-free minute), confirm that the 3-in-24 pattern error detector is operating.

6. Type **`test ds1-loop`** ***`XXXVS`*** **`inject-single-bit-error`**

   where ***`XXX`*** is the administered number of the G700 or G350 (for example, **002**), and ***`VS`*** is the slot number on the G700 or G350 of the Media Module (for example, **V3**).

7. Type **`list meas ds1 sum`** ***`XXXVS`*** to display the bit error count again.
8. Step through Table 6: DS1 Bit-error count troubleshooting on page 85 to troubleshoot.

Table 6: DS1 Bit-error count troubleshooting

Condition	Solution
The value of the **Bit-error count** field is greater than `1`	Replace the ICSU, and retest.
The value of the **Bit-error count** field is still greater than `1` after you replace the ICSU	Replace the DS1 circuit pack, and retest.
The value of the **Bit-error count** field is `1`	The test passed.

9. Type **`test ds1-loop`** ***`location`*** **`end-loopback/span-test`** to end the test.

   Wait about 30 seconds for the DS1 to reframe on the incoming signal and clear DS1 facility alarms. Use Table 7: Evaluation of DS1 loopback test results on page 86 to evaluate the test results and to determine the solution.

Table 7: Evaluation of DS1 loopback test results

Condition	Solution
Loopback termination fails with an error code of 1313.	The span is still looped somewhere, possibly at the loopback jack, at the ICSU, or somewhere in the network.
The red LED on the loopback jack is on.	Replace the ICSU, and re-run the test.
Loopback termination still fails.	Replace the DS1 circuit pack, and repeat the test
The DS1 cannot frame on the incoming span's signal after the loopback jack power down.	There is something wrong with the receive signal into the loopback jack from the dumb block or the smart jack.
The span failed the service provider's loopback test.	The problem is in the service provider's network.
The service provider successfully loop tested the span, up to the smart jack.	The wiring between the loopback jack and the smart jack is suspect. Test, and make repairs, as needed.
You cannot locate and repair the problem in the time available and must terminate the test.	The test will not terminate normally in the absence of a good framing signal. You have to reset the circuit pack. Enter **`reset board`** ***`XXXVS`***.
The test terminated normally.	Proceed with To restore DS1 administration on page 86.

To restore DS1 administration

1. At the SAT, type **`change ds1`** ***`XXXVS`*** to open the **DS1 administration** form.
2. Go to page 2 of the **DS1 administration** form.
3. Change the value of the **TX LBO** field to the original value that you wrote down when you were administering the DS1 for the test.
4. Press **ENTER** to save the changes.

To release the DS1 circuit pack

1. At the SAT, type **`release board`** ***`XXXVS`***.

2. Leave the loopback jack in place.

Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer (MUX)

To test the DS1 span from the smart jack to the CO:

1. Have the service provider run a smart-jack loopback test against the network interface wiring that links the smart jack to the CO (section 3 in Figure 4: Network interface at smart jack for an MM710 multi-media module on page 88through Figure 6: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module on page 90).
2. If the tests fails, there is a problem on the network side.

   Have the service provider correct it.

Testing the DS1 span from the loopback jack to the smart jack

Note:

> This test cannot isolate the problem if there are problems in the wiring between the far-end CO and the far-end ICSU. You must coordinate this test with the DS1 service provider.

Test the short length of customer premises wiring between the loopback jack and the smart jack (Section 2 in the following 3 figures) using a loopback that overlaps this section of the span.

To test the DS1 span from the loopback jack to the smart jack:

1. Have the DS1 service provider at the CO end run a local ICSU line loopback test.
2. Have the DS1 service provider at the CO end run a local DS1 payload loopback test.
3. Run a far-end MM710 line loopback, using the following procedure:
   a. From the SAT, type **`test ds1-loop`** ***`XXXVS`*** **`far-csu-loopback-test-begin`**

      where ***`XXX`*** is the administered number of the G700 (for example, **002**), and ***`VS`*** is the slot number on the G700 of the Media Module (for example, **V3**).

   b. Examine the bit-error counts, as in Testing the integrity of data sent over the loop on page 84.

   c. Type **`test ds1-loop`** ***`location`*** **`end-loopback/span-test`** to terminate the test.

If the test fails and the there were no problems when Testing the DS1 span from the ICSU to the loopback jack or Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer (MUX), there is a problem between the loopback jack to the smart jack. Work with the service provider to isolate the fault.

Figure 4: Network interface at smart jack for an MM710 multi-media module

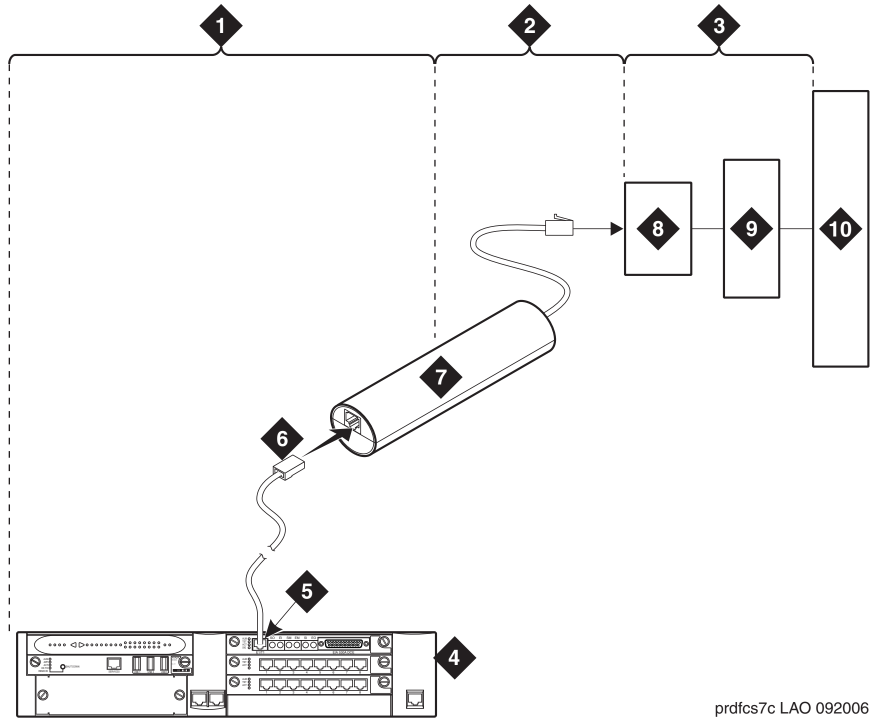


Figure notes:

1. Span section 1
2. Span section 2
3. Span section 3
4. G700 or G350 Media Gateway
5. E1/T1 port on an MM710 multi-media module
6. RJ-48 to network interface (up to 1000 ft. [305 m])
7. Loopback jack
8. Network interface smart jack
9. Interface termination or fiber multiplexer (MUX)
10. Central office

Figure 5: Network interface at extended demarcation point (smart jack inaccessible) for an MM710 multi-media module

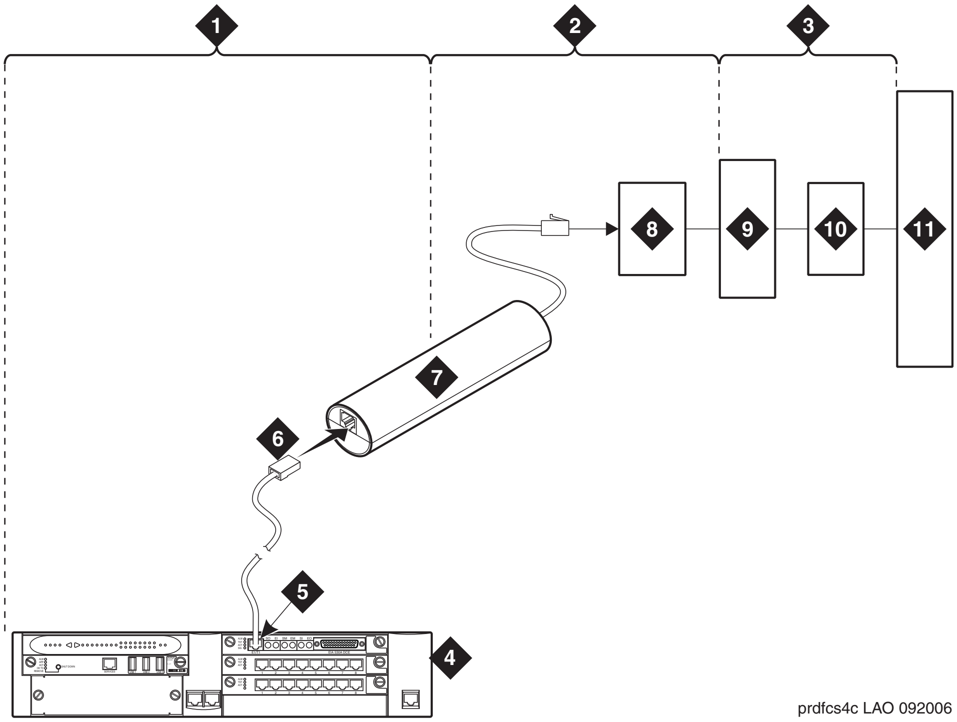
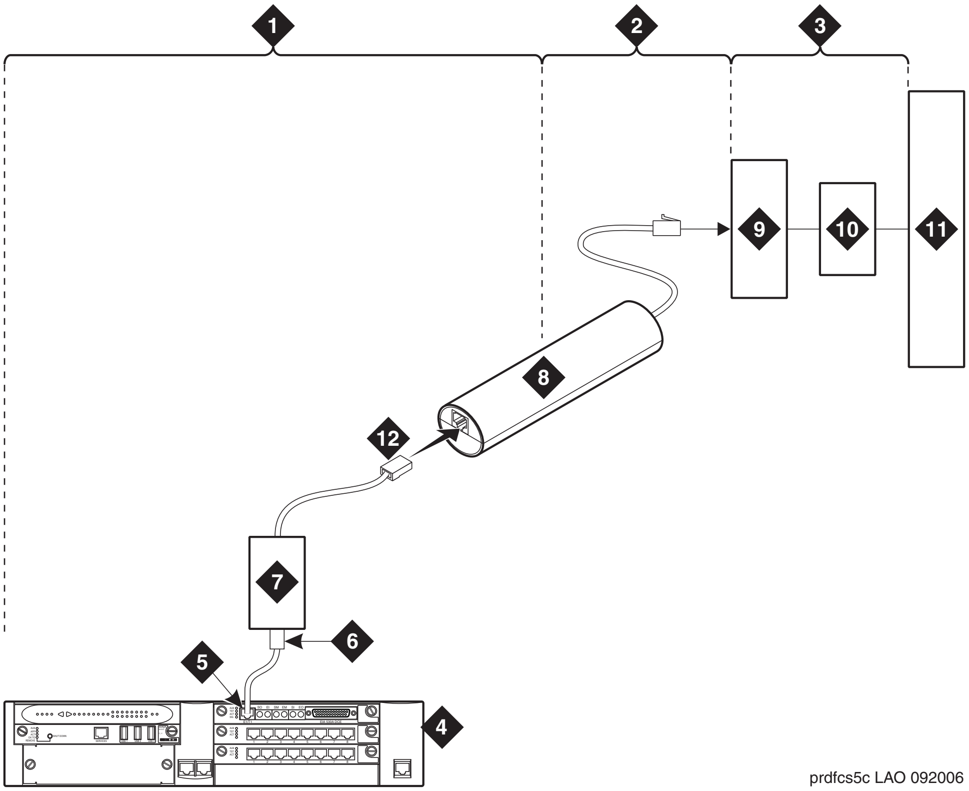


Figure notes:

1. Span section 1
2. Span section 2
3. Span section 3
4. G700 or G350 Media Gateway
5. E1/T1 port on an MM710 multi-media module
6. RJ-48 to network interface (up to 1000 ft. [305 m])
7. Loopback jack
8. Dumb block (extended demarcation)
9. Network interface smart jack
10. Interface termination or fiber multiplexer (MUX)
11. Central office

Figure 6: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module



prdfcs5c LAO 092006

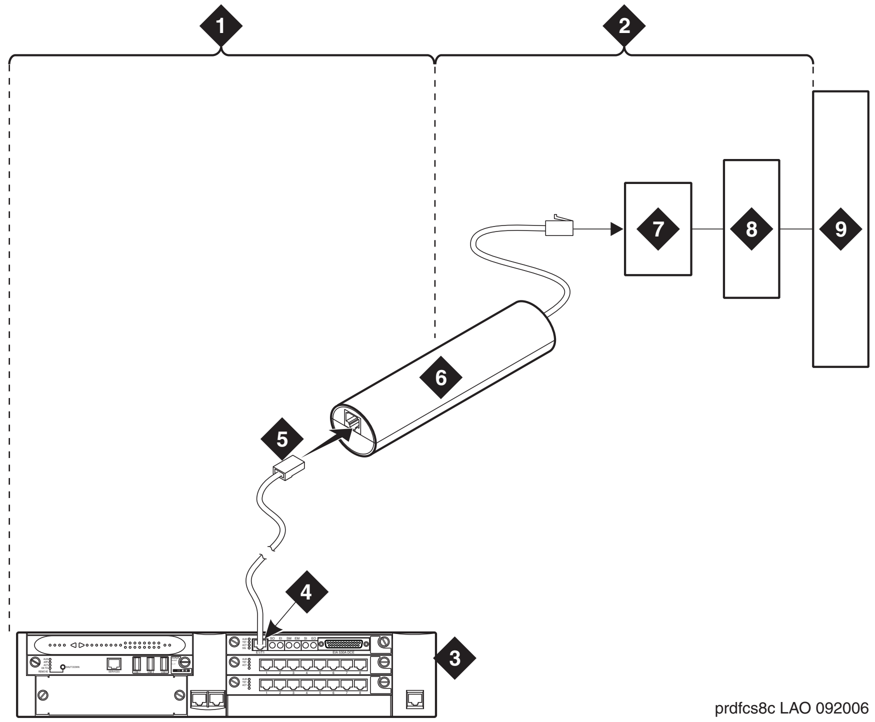
Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **Span section 3**
4. **G700 or G350 Media Gateway**
5. **E1/T1 port on an MM710 multi-media module**
6. **RJ-48 to network interface (up to 1000 ft. [305 m])**
7. **Dumb block (extended demarcation)**
8. **Loopback jack**
9. **Network interface smart jack**
10. **Interface termination or fiber multiplexer (MUX)**
11. **Central office**
12. **Dumb block to smart jack RJ-48**

Testing a loopback jack without a smart jack

When the loopback jack is added to a span that does not contain a smart jack, the span is divided into 2 sections: from the MM710 to the loopback jack and from the loopback jack to the central office (CO). Section 2 includes the short cable from the loopback jack to the dumb block demarcation point (part of the loopback jack). This cable is the only part of Section 2 that is part of customer premises wiring. It is not covered in the loopback jack's loopback path. See Figure 7: Network interface at "dumb" block for an MM710 multi-media module on page 91 and Figure 8: Network interface at "dumb" block with repeater line to fiber MUX for an MM710 multi-media module on page 92.

Figure 7: Network interface at "dumb" block for an MM710 multi-media module



prdfcs8c LAO 092006

Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **G700 or G350 Media Gateway**
4. **E1/T1 port on an MM710 multi-media module**
5. **RJ-48 to network interface (up to 1000 ft. [305 m])**
6. **Loopback jack**
7. **Dumb block (demarcation point)**
8. **Interface termination or fiber multiplexer (MUX)**
9. **Central office**

Figure 8: Network interface at “dumb” block with repeater line to fiber MUX for an MM710 multi-media module

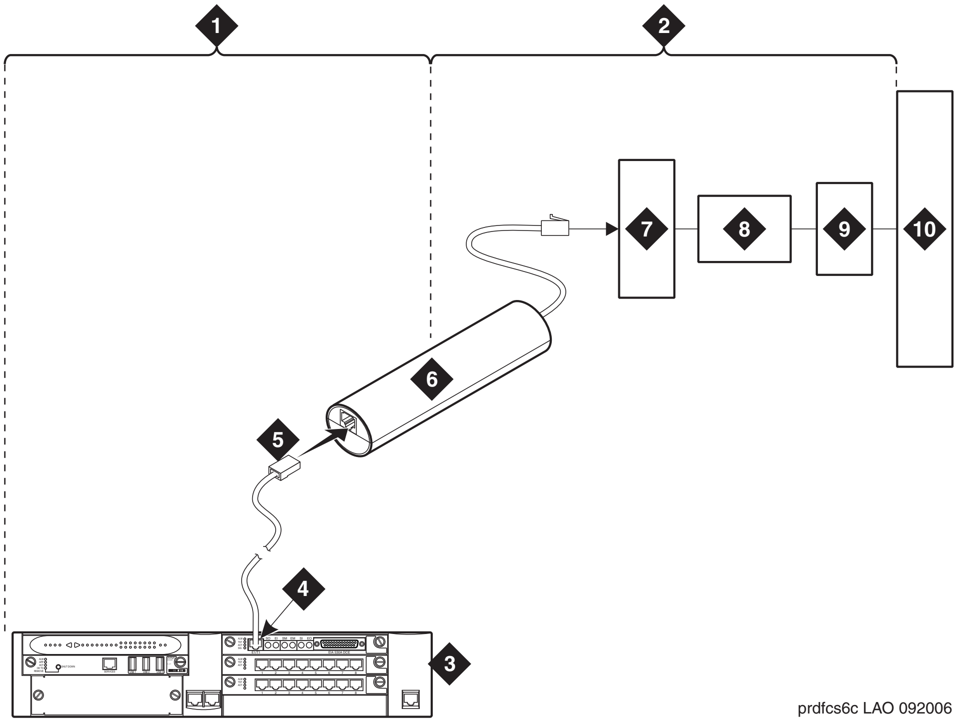


Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **G700 or G350 Media Gateway**
4. **E1/T1 port on an MM710 multi-media module**
5. **RJ-48 to network interface (up to 1000 ft. [305 m])**
6. **Loopback jack**
7. **Dumb block (demarcation point)**
8. **Repeater**
9. **Fiber multiplexer (MUX)**
10. **Central office**

You are responsible for finding and correcting problems in the customer wiring (section 1 and the loopback cable portion of section 2). The DS1 service provider is responsible for finding and correcting problems in the majority of section 2.

To test a loopback jack without a smart jack

1. Test customer premises wiring from the MM710 to the loopback jack, as described in Testing the DS1 span from the loopback jack to the smart jack on page 87.
2. Test the loopback jack-to-*dumb* block and *dumb* block-to-CO wiring (section 2 in Figure 7: Network interface at “dumb” block for an MM710 multi-media module on page 91 and Figure 8: Network interface at “dumb” block with repeater line to fiber MUX for an MM710 multi-media module on page 92).

   This can be done using a loopback that “overlaps” the section of the span. Any of the following loopbacks can do this:

   - The local ICSU’s line loopback, which the DS1 service provider at the CO end typically activates, tests, and then deactivates.
   - The local DS1 interface’s payload loopback, which the DS1 service provider at the CO end activates and tests.
   - The far-end MM710’s line loopback:
     a. At the SAT type **`test ds1-loop`** ***`location`*** **`far-csu-loopback-test-begin`** to activate this test,

        where ***`location`*** is the DS1 interface circuit pack corresponding to the loopback jack.

     b. Type **`test ds1-loop`** ***`location`*** **`end-loopback/span-test`** to terminate this test,

        where ***`location`*** is the DS1 interface circuit pack corresponding to the loopback jack.

   Bit error counts are examined as described in Testing the DS1 span from the ICSU to the loopback jack on page 82. This test only isolates problems to Section 2 wiring if there are no problems in the wiring between the far-end CO and the far-end ICSU. Coordinate this test with the DS1 service provider.

   Failure of any of these tests indicate a problem in Section 2. This could mean bad loopback jack -to-”dumb” block cabling, but is more likely to indicate a problem somewhere between the “dumb” block and the CO. This is the responsibility of the DS1 service provider.

   If the DS1 Span Test confirms that there are no problems in Section 1, the technician should proceed as follows to avoid unnecessary dispatch:

   a. Identify and contact the DS1 service provider.

   b. Inform the DS1 provider that loopback tests of the CPE wiring to the “dumb” block (section 1) showed no problems.

   c. If the far-end MM710 line loopback test failed, inform the DS1 provider.

   d. Request that the DS1 provider perform a loopback test of their portion of the Section 2 wiring by sending someone out to loop Section 2 back to the CO at the “dumb” block.

   If this test fails, the problem is in the service provider’s wiring.

   If the test passes, the problem is in the cable between the loopback jack and the “dumb” block. Replace the loopback jack.

Configurations using fiber multiplexers

Use the loopback jack when customer premises DS1 wiring connects to an on-site fiber multiplexer (MUX) and allows wiring to the network interface point on the MUX to be remotely tested. This requires that the MM710 CSU be set so it can be used on DS1 wiring to the MUX.

Fiber MUXs can take the place of Interface termination feeds as shown in Figure 4: Network interface at smart jack for an MM710 multi-media module on page 88 through .Figure 7: Network interface at “dumb” block for an MM710 multi-media module on page 91 Test these spans using the same procedures as metallic spans.

Note:

Fiber MUXs may have loopback capabilities that the service provider can activate from the CO end. These may loop the signal back to the CO or back to the DS1 MM710. If the MUX provides the equivalent of a line loopback on the “problem” DS1 facility, activate it after a successful loopback jack test, and use it to isolate problems to the wiring between the loopback jack and the MUX.

⚠ **Important:**

Be aware that there are installations that use repeater-augmented metallic lines between the MUX and the “dumb” block. These lines require DC power for the repeaters and this DC power is present at the “dumb” block interface to the CPE equipment. *A loopback jack is required in this configuration to properly isolate and terminate the DC power.*

Checking for the presence of DC

To check for the presence of DC:

1. Make the following four measurements at the network interface jack:
   a. From transmit tip (T, Pin 5) to receive tip (T1, Pin 2)
   b. From transmit ring (R, Pin 4) to receive ring (R1, Pin 1)
   c. From transmit tip (T, Pin 5) to transmit ring (R, Pin 4)
   d. From receive tip (T1, Pin 2) to receive ring (R1, Pin 1)

All measurements should read 0 (zero) volts DC. For pin numbers and pin designations, refer to *Integrated Channel Service Unit (ICSU) Installation and Operation*.

External modems

The following section assumes that you are using one of the recommended external modems. However, any locally obtained, type-approved external modem should work. Contact your Avaya representative for more information.

Recommended modems include:

- USB US Robotics Modem 5637-OEM
- MultiTech MT9234ZBA-USB
- Recommended Modems (Discontinued)

This section covers:

- Hardware required when configuring modems on page 95
- Recommended Modems on page 96
- MT9234ZBA-USB on page 96
- Administering Multi-Tech modems on page 96

Hardware required when configuring modems

To configure many modems, you use the Hayes-compatible AT command set.

Note:

Note:

If your modem uses a USB connection, use the USB ports instead of the serial port. Also, AT commands are not required, so you can skip this section. Use the factory defaults.

Before you can enter AT configuration commands, you must first connect a terminal or a PC with a keyboard, monitor, and terminal-emulation software to the modem.

Proceed as follows:

1. Connect one end of an RS-232 cable to an RS-232, serial-communications port (often called a COM port) on the terminal or PC.
2. Connect the other end of the RS-232 cable to the modem.
3. If you are using a PC, start your terminal emulation software.

Recommended Modems

Avaya recommends using a MultiTech MT9234ZBA-USB or a USB US Robotics Modem 5637-OEM with an S8300/G700, S8500, or S8700/S8710 configuration. The modem is used for sending alarms, as well as for remote dial up to the server for maintenance and administration.

The modem model MT5634ZBA-USB-V92 is discontinued.

Configuring the MT9234ZBA-USB modem

In the United States, the MT9234ZBA-USB modem gets configured automatically through the USB port with the factory defaults. No special configuration is necessary. In a non-US country, the modem may require settings specific to the country in which the modem will be used.

MT9234ZBA-USB

Avaya recommends using a MultiTech modem, model MT9234ZBA-USB-V92-GLOBAL, with a G350 media gateway.

The Multi-Tech serial modem connects the G350 media gateway to an external trunk. This connection enables remote dial in capability for administration and troubleshooting. For more information, see *Installing and Upgrading the Avaya G350 Media Gateway,* 03-300394.

Administering Multi-Tech modems

The Multi-Tech modems do not require administration if used in the United States. In non-US countries, these modems may require administration.

For the full range of modem options, see the *Administering Avaya Aura™ Communication Manager*, 03-300509.

Busy tone disconnect equipment for non-U.S. installations

The customer-provided busy tone disconnect adjunct detects busy tone disconnects of incoming calls on loop-start, 2-wire, analog trunks. In some non-U.S. countries where a G700 or G350 Media Gateway is used, the PSTN sends busy tone as the disconnect signal. Therefore, the S8300 Server, G700 Media Gateway, or G350 Media Gateway requires a busy tone disconnect adjunct. Figure 9 shows typical connections.

Figure 9: Typical cabling for busy tone disconnect

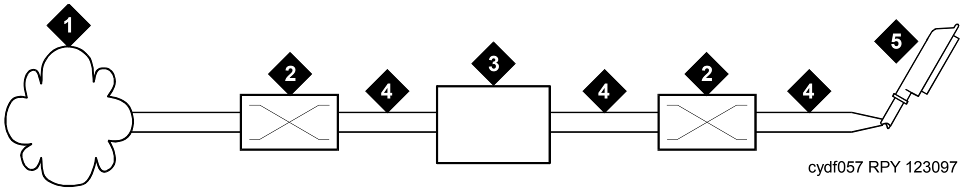


Figure notes:

1. **Public switched telephone network**
2. **Main distribution frame**
3. **Busy tone disconnect device**
4. **Tip and ring wires**
5. **To loop-start, central-office, trunk MM711 analog media module**

Music-on-hold

The music-on-hold (MOH) feature allows a caller to hear music when that caller is placed on hold. This section covers:

- Installing an unregistered music source on a G700 or G350 Media Gateway on page 98
- Installing a registered music source on a G700 or G350 Media Gateway on page 101

Music-on-hold can be provided:

- Through a port on an MM711 Analog Media Module to a customer-supplied music source on a G700 Media Gateway
- Through a port on an MM711 Analog Media Module or MM714 Analog Media Module, or through a fixed analog port (LINE 1 or LINE 2) to a customer-supplied music source on a G350 Media Gateway

On a G700 or G350 Media Gateway, the music-on-hold feature is connected through a port on an MM711 Analog Media Module or, for a G350 Media Gateway only, an MM714 Analog Media Module, or the analog LINE ports of the integrated analog media module.

The G700 or G350 Media Gateway does not support an auxiliary trunk circuit pack. Therefore, for S8300 Server users, the music-on-hold feature through an auxiliary trunk is not supported. However, G700 or G350 Media Gateway users with an S8500 or S8700-series Server as primary controller can access the music-on-hold feature, if their equipment is physically connected to a TN763 auxiliary trunk circuit pack in an EPN carrier of an S8500 or S8700-series system.

Installing an unregistered music source on a G700 or G350 Media Gateway

Figure 10 and Figure 11 show the connections for the music-on-hold feature on a G700 Media Gateway for an unregistered source.

Note:

The G350 Media Gateway's physical connection with the MM711 Analog Media Module, MM714 Analog Media Module, or fixed analog ports (LINE 1 or 2) on the front panel is the same as the G700 Media Gateway's connection with the MM711 Analog Media Module.

Note:

If you want multiple music sources, you must use multiple ports on the MM711 Analog Media Module.

Figure 10: Unregistered music-on-hold equipment connecting to KS-23395-L3 for a G700 Media Gateway

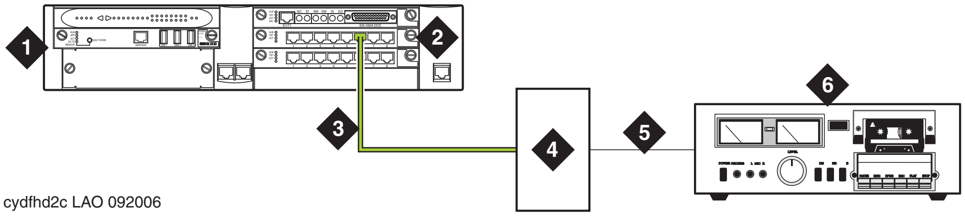


Figure notes:

1. **G700 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **KS-23395-L3 coupler**
5. **RCA cord**
6. **Music source**

To connect an unregistered music-on-hold source to a G700 or G350 Media Gateway using a KS-23395-L3 coupler:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.

   For a G350 Media Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.

2. Connect the other end of the RJ-45 cable to a KS-23395-L3 coupler.

3. Connect the KS-23395-L3 coupler to the customer-supplied music source.

   Follow the manufacturer's instructions to properly connect the music source to the KS-23395-L3 coupler. Normally, you simply use an RCA cord.

4. Administer the switch for the new equipment.

Figure 11: Unregistered music-on-hold equipment connecting to KS-23395-L4 for a G700 Media Gateway

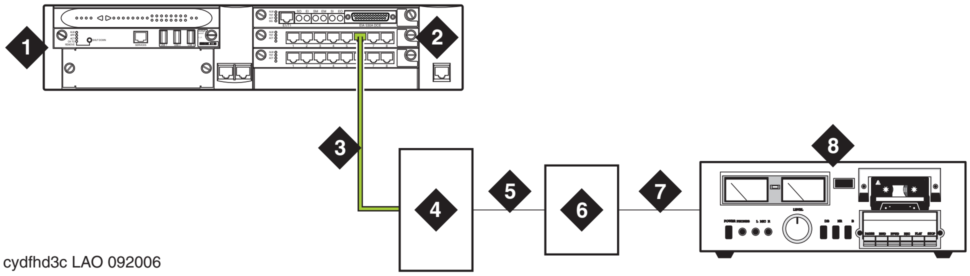


Figure notes:

1. **G700 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **KS-23395-L4 coupler**
5. **8-pair modular cord**
6. **909A/B universal coupler**
7. **8-pair modular cord**
8. **Music source**

To connect an unregistered music-on-hold source to a G700 or G350 Media Gateway using a KS-23395-L4 coupler:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.

   For a G350 Media Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the other end of the RJ-45 cable to a KS-23395-L4 coupler.
3. Connect the KS-23395-L4 coupler to the 909A/B universal coupler using a 8-pair modular cord.
4. Connect the 909A/B universal coupler to the music source using a 8-pair modular cord.
5. Administer the switch for the new equipment.

Note:

Note: For additional installation information, refer to *909A/909B Universal Coupler Installation Instructions*, which is normally shipped with the 909A/909B Universal Coupler.

Installing a registered music source on a G700 or G350 Media Gateway

Figure 12 show the connections for the music-on-hold feature on a G700 Media Gateway for a registered source.

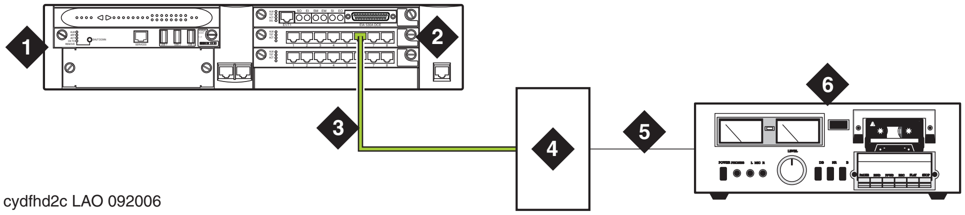
Note:

The G350 Media Gateway's physical connection with the MM711 Analog Media Module, MM714 Analog Media Module, or fixed analog ports (LINE 1 or 2) on the front panel is the same as the G700 Media Gateway's connection with the MM711 Analog Media Module.

Note:

If you want multiple music sources, you must use multiple ports on the MM711 Analog Media Module.

Figure 12: Registered music-on-hold equipment connecting to KS-23395-L4 for a G700 Media Gateway



cydfhd2c LAO 092006

Figure notes:

1. **G700 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **KS-23395-L4 coupler**
5. **8-pair modular cord**
6. **Music source**

To connect a registered music-on-hold source to a G700 or G350 Media Gateway using a KS-23395-L4 coupler:

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.

   For a G350 Media Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.

2. Connect the KS-23395-L4 coupler to the customer-supplied music source.

   Normally, you simply use a 8-pair modular cord.

3. Administer the switch for the new equipment.

Paging and announcement equipment

This section provides information on loudspeaker paging.

On a G700 or G350 Media Gateway, the loudspeaker paging feature is connected through a port on an MM711 Analog Media Module. The port is administered on the SAT Station screen, not the Loudspeaker Paging screen.

The G700 or G350 Media Gateway does not support an auxiliary trunk circuit pack. Therefore, the loudspeaker feature through an auxiliary trunk is not supported on a G700 or G350 Media Gateway.

Users on a G700 or G350 Media Gateway controlled by an S8700/S8710 or S8500 can also access the loudspeaker paging feature if equipment is physically connected to a TN763 auxiliary trunk circuit pack in an PN carrier of an the S8700/S8710 or S8500 system.

Figure 13 shows the connections for loudspeaker paging, dial dictation, or recorded announcement features on a G700 or G350 Media Gateway.

Figure 13: Typical loudspeaker equipment connections for a G700 or G350 Media Gateway

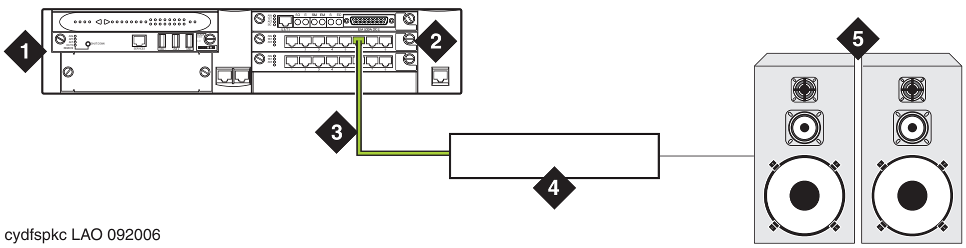


Figure notes:

1. **G700 or G350 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **Telephone hybrid (third party) device**
5. **Loudspeaker paging system**

To hook up loudspeaker paging from a G700 or G350 Media Gateway

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.
2. Connect the other end of the RJ-45 cable to a customer-supplied telephone hybrid device.
3. Follow the manufacturer's instructions to properly connect the telephone hybrid device to your loudspeaker paging system.
4. Administer the M711 port on the SAT Station screen as an analog station.

Note:

Do not administer the MM711 port on the SAT Loudspeaker Paging screen.

Adjunct Information Sources

This section lists documents you can use for installation of some of the key adjunct systems that you can connect. This section covers:

- Call Management System
- Communication Manager Messaging Systems
- Avaya Modular Messaging System
- ASAI and DEFINITY LAN Gateway
- Avaya Interactive Response
- Avaya EC500 Extension to Cellular and Off-PBX Stations
- SIP Enablement Services
- Seamless Converged Communications across Networks (SCCAN)
- Call Accounting Systems

Call Management System

For information on installing Call Management System R3V12, see the following:

- *Avaya Call Management System (CMS) R12 Software Installation, Maintenance, and Troubleshooting Guide* (585-215-117)
- *Avaya Call Management System (CMS) Sun Enterprise 3500 Computer Hardware Installation, Maintenance, and Troubleshooting* (585-215-873)
- *Avaya CMS R12 Sun Blade 100/150 Workstation Hardware Installation, Maintenance, and Troubleshooting* (585-215-783)
- *Avaya CMS Sun Fire V880 Computer Hardware Installation, Maintenance, and Troubleshooting* (585-215-116)

Communication Manager Messaging Systems

For information on installing Communication Manager Messaging systems, see one of the following:

Note:

Starting with Communication Manager release 5.2, IA770 is called CM Messaging.

- For INTUITY AUDIX LX Messaging, see *INTUITY AUDIX LX Installation Checklist* on the *INTUITY AUDIX LX Release 1 Documentation CD-ROM*, 585-313-818.
- For Communication Manager Messaging Release 5.2, *Avaya Aura* ™ *Communication Manager Messaging Release 5.2 Installation and Initial Configuraton.*

Avaya Modular Messaging System

For information on installing Avaya Modular Messaging systems, see *Modular Messaging Release 4.0 Documentation CD-ROM*, 11-300121.

ASAI and DEFINITY LAN Gateway

For information on installing ASAI systems and DEFINITY LAN Gateway, see Avaya *MultiVantage ASAI Applications over MAPD*, 555-230-136 and *Avaya Communication Manager Release 2.0 ASAI Technical Reference*, 555-230-220 on the *Avaya Communication Manager Release 2.0 ASAI Documents* CD-ROM, 585-246-801.

Another document related to ASAI is *Avaya CVLAN Server 9.0 for Linux Installation and Basic Administration*, which is available at http://avaya.com/support. Click the following links: **Support>Technical Database>Contact Centers/CRM>CTI>CVLAN Server for Linux R9**.

Avaya Interactive Response

For information on installing Avaya Interactive Response systems, see *Avaya Interactive Response R1.3 Installation, Migration, and Troubleshooting Guide* (07-300180) on the *Avaya Interactive Response R1.3 Documentation CD* (07-300181).

Avaya EC500 Extension to Cellular and Off-PBX Stations

For information on installing Avaya EC500 Extension to Cellular and Off-PBX Station systems, see the *Avaya EC500 Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide*, 210-100-500.

SIP Enablement Services

For information on installing Avaya SIP Enablement Services (SES), see the *Avaya Aura™ SIP Enablement Services Implementation Guide*, 16-300140, and *SIP Support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers*, 555-245-206.

Seamless Converged Communications across Networks (SCCAN)

For information on installing Seamless Converged Communications across Networks (SCCAN), see the *SCCAN Total Solution Guide*, 21-300041, and the *SCCAN Configuration Guide*. Additionally, see the following:

- *Avaya W310 WLAN Gateway Installation and Configuration Guide*, 21-300041
- *Avaya W310/W110 Quick Setup Guide Using the CLI,* 21-300178
- *Avaya W310/W110 Quick Setup Guide Using the W310 Device Manager,* 21-300179
- *Wireless AP-4, AP-5, and AP-6 User Guide*, 555-301-708, Issue 3
- *Motorola NMS User Guide*
- *Motorola WSN User Guide*

Call Accounting Systems

For information on installing Call Accounting Systems, see the online help or documentation included with the eCAS software CD-ROM.

Section 2: S8300 Server installation and upgrades

This section contains procedures to install or upgrade an Avaya S8300-Series Server, using one of the available Avaya wizard tools.

Installing S8300 Server using Avaya Installation Wizard release 5.2

About Avaya Installation Wizard

Avaya Installation Wizard is installed with Communication Manager Software. Hence, the release version of Avaya Installation Wizard and Communication Manager are the same. For example, with Communication Manager release 5.2, the release of Avaya Installation Wizard is 5.2.

Using the Avaya Installation Wizard R5.2

- Install an S8300 Server as a Main Server or as an LSP (Local Survivable Server)

Upgrading S8300 Server

Upgrade Communication Manager release 5.1.X or earlier on an S8300 Server to release 5.2, by using any of the following methods:

- Software Update Manager
- Manage Software Web page

> ⚠ **Important:**
> You cannot use the following tools to upgrade Communication Manager release 5.1.X or earlier to release 5.2:

- Avaya Installation Wizard
- Upgrade Tool

  However, to upgrade to a pre-5.2 release, use the Avaya Installation Wizard or the Upgrade Tool available with Communication Manager pre-5.2 releases.

Related Documentation

Please search for the latest versions of the documents from http://support.avaya.com:

- Avaya Installation Wizard, http://support.avaya.com/avayaiw

  See *Job Aid: Avaya Installation Wizard,* 555-245-754.
- Software Update Manager

  See *Avaya Integrated Management 3.3 Software Update Manager User Guide*, 14-601743.

Note:

These tools replace many normal installation or upgrade procedures in this section. However, they do not automate all of the tasks associated with an installation or an upgrade. When you have to perform a task manually, the required information is mentioned in the subsequent chapters of this section.

This section is organized into the following chapters:

- Chapter 3: Installing a new S8300 using the Avaya Installation Wizard
- Chapter 4: Upgrading Communication Manager on an existing S8300B or S8300C Server on page 203

Note:

Manual procedures to perform these tasks are available in Section 3: Manual procedures to install and upgrade an S8300 Server.

Chapter 3: Installing a new S8300 using the Avaya Installation Wizard

This chapter covers the procedures to install a new Avaya S8300 Server. The S8300 can be configured as either the primary controller or as a local survivable processor (LSP).

The new S8300 normally ships ***without any software on its hard drive***. To install the software, you need to have an external USB DVD or CD-ROM drive.

If the S8300 is configured as an LSP, the primary controller, running Communication Manager, can be either another S8300, or an S8400, S8500, or S8700-series Server.

Note:

Procedures to install or upgrade an S8400, S8500, or S8700-series Server are not covered in this document. See *Documentation for Avaya Aura™ Communication Manager, Media Gateways and Servers*, which is on the Avaya Support web site (http://www.avaya.com/support) or on the CD, 03-300151.

The steps to install an S8300 configured as an LSP are the same as the steps to install an S8300 configured as the primary controller, with the following additional considerations:

- The version of Communication Manager on the LSP must be the same as, or later than, the version running on the primary controller.
- For an LSP, you administer Communication Manager translations on the primary controller, *not* on the LSP. The primary controller then copies the translations to the LSP.
- An LSP *cannot* have SIP Enablement Services (SES) enabled.
- An LSP must be configured as XL if the primary controller is an S8720 Server in an XL configuration or an S8730 Server. Administer this option on the Configure Server — Configure LSP Web page.

⚠ **Important:**

The Avaya Installation Wizard (IW) is used to configure the server (Using the Avaya Installation Wizard (IW) on page 126) and install firmware on the media gateway after the Communication Manager software is installed. Other tasks have to be done manually, and are identified in the sections to follow.

Installation Overview

About software and firmware files

The hard drive is blank on a new S8300B server. The hard drive and internal CompactFlash are blank on a new S8300C or S8300D server. It may be necessary to install a service pack on the S8300 after installing the Communication Manager software, and/or to upgrade the media gateway and media module firmware.

Communication Manager software is distributed on a CD-ROM that you take to the site. Additional files that may be needed are the most recent versions of the software service pack file and the media gateway firmware files. You may need to obtain these files from the Avaya Support web site.

About access to the Communication Manager software distribution CD

The R5.2 Communication Manager software and other files needed for the R5.2 installation are on the Communication Manager software distribution CD that you take to the customer site. Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate.

This chapter describes the upgrade procedure using the CD-ROM drive as source of the software.

About SIP Enablement Services and Communication Manager Messaging software

SIP Enablement Services (SES) and Communication Manager Messaging software is also stored on the Communication Manager software distribution CD-ROM.

SES software is automatically installed on the S8300 Server when you install Communication Manager. For SES to be administered and operational, you must enable SES software and install an SES-specific license after the software is installed.

Communication Manager Messaging software is optionally installed on the S8300 Server when you install Communication Manager. If the customer does not want to use Communication Manager Messaging, do not install Communication Manager Messaging software.

⚠ **CAUTION:**

If Communication Manager Messaging (CMM) is not installed along with Communication Manager, then CMM can be installed at a later time. In this case, you run an upgrade of the server using Manage Software web page, choose the same software that the server is already running, and select Communication Manager Messaging for installation during the upgrade.

Tasks to install the S8300 and a media gateway

Before going to the customer site

- Obtaining a USB DVD or CD-ROM drive on page 113
- Obtaining information that the project manager provides on page 113
- Obtaining service pack files, if needed on page 115
- Obtaining service pack and language files for Communication Manager Messaging, if necessary on page 116
- Completing the RFA process (Obtaining license and authentication files) on page 117
- Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary on page 118

Install the S8300

- Inserting the S8300 on page 120
- Accessing the S8300 on page 121
- Installing Communication Manager Software on page 122
- Verifying Software Version on page 124
- Creating a super-user login on page 124
- Using the Avaya Installation Wizard (IW) on page 126
- If you set date or time, reboot the server on page 163
- If the server is an LSP, stop and start Communication Manager on page 163
- Enabling SIP Enablement Services, if required on page 164

Administer an S8300 primary controller

- Assigning node names and IP addresses for the LSPs on page 166
- Administering Network Regions on page 166
- Associating LSPs with Network Regions on page 171
- Administering IP Interfaces on page 169

- Identifying LSPs to the S8300 primary controller on page 170

Administer an S8400, S8500, or S8700-series primary controller

- Assigning Node Names and IP Addresses for the C-LANs and LSPs on page 173
- Administering Network Regions on page 173
- Assigning LSPs with Network Regions on page 182
- Administering IP Interfaces on page 177
- Identifying the Survivable Processor on the primary controller on page 181

Administer the media gateway

- Administering the Media Gateway with S8300 Server on page 182
- Saving Communication Manager translations on page 186

Administer CM Messaging

- If using CM Messaging, administer Communication Manager for CM Messaging on page 187

Administer SES

- Installing the SES license on page 187
- SES administration tasks on page 189

IP phones considerations

- Considerations for IP Phones Supported by a Local Survivable Processor on page 190

Transition from Primary Controller to LSP

- Transition of Control from Primary Controller to LSP on page 192

Complete the installation of the S8300 (if the primary controller)

- Reboot the server on page 194
- Integrity check on page 194
- Updating Communication Manager Messaging, if installed on page 195
- Backing up system data on page 198

Complete the installation of the S8300 (for an LSP)

- Complete the Installation Process (for an S8300 LSP) on page 201

Final Tasks

- Final tasks on page 201

Before going to the customer site

The procedures in this section should be completed before going to the customer site or before starting a remote installation.

Obtaining a USB DVD or CD-ROM drive

Installing Communication Manager on an S8300 requires remastering the S8300 hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB DVD or CD-ROM drive. Therefore, you must have a USB DVD or CD-ROM drive at the site.

Obtaining information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. The following worksheets contain the setup information:

- Electronic pre-installation worksheet
- Name and number list
- Custom template

Information on how to use these files is contained within the files themselves.

Electronic pre-installation worksheet

The Electronic Pre-Installation Worksheet (EPW) is filled in by the customer or by the project manager, the software specialist, or another support person who configures Voice over IP systems. The data from this worksheet is automatically pulled into Avaya Installation Wizard to configure the servers and gateways.

Name and number list

The Name and Number List, like the EPW, is an Excel spreadsheet. The Name and Number List contains administration data for multiple users. The IW pulls this data to automatically administer users on the new system. This administration includes users' names, unicode names (for native names in Chinese, Japanese, and other non-ASCII character languages), extensions, telephone types, classes of service, languages, locations, and voice mail capability.

The Name and Number List also includes hunt group port configuration for a new Communication Manager Messaging systems.

⚠ **CAUTION:**

> For the Avaya Installation Wizard to install an Communication Manager Messaging system, you *must* complete the subscriber data on the Name and Number List and then use the Name and Number List with the Avaya Installation Wizard.

As each user's name and accompanying data is imported, the wizard will administer the station using the provided information along with default values for other station fields. After the import has completed, each station will be ready to be plugged into the wall jack and activated. Analog and digital phones will be ready for a TTI registration sequence. IP phones will be ready for an IP registration sequence.

The default values used by the wizard can be viewed at http://support.avaya.com/avayaiw under the **Avaya Installation Wizard Default Parameters** link. If the wizard defaults do not meet the customer's needs, you can use a custom template.

Custom template

The Custom Template is a third Excel spreadsheet that allows automatic administration of key custom Communication Manager translations. These are:

- Classes of Service
- Feature Access Codes
- Trunk Access Codes
- Telephone button assignments
- TTI codes
- Voice mail hunt group number and coverage path

Obtaining the Serial Number of the media gateway, if necessary

For a new installation of a media gateway with an S8300, you need the serial number of the media gateway in order to complete the creation of the customer's license file on the rfa.avaya.com web site. To get this number, look for the serial number sticker on the back of the chassis of the media gateway. If the unit is delivered directly to the customer and you will not have phone or LAN line access from the customer site to access the rfa.avaya.com web site, this task will require a preliminary trip to the customer site.

Checking for an FTP/SCP/SFTP Server or Compact Flash for Backing up Data

During the installation and upgrade procedures, you can back up the S8300 data to an FTP, SFTP, or SCP server connected through the customer's LAN, or to the USB Compact Flash drive (S8300C or S8300D only). If you plan to back up data on a customer's LAN, use a server on the customer's LAN.

Note:

Only specific releases of Communication Manager allow back up to an SFTP or an SCP Server.

- Check with your project manager or the customer for the following information about theFTP, SFTP, or SCP server.
  - Login ID and password
  - IP address
  - Directory path on the FTP Server

⚠ **Important:**

Before going to the customer site, make sure that either a customer server or a compact flash card will be available to store system backups.

Obtaining service pack files, if needed

If one or more service packs are required for this installation or upgrade procedure, and the service pack files are not on your software CD, download the service pack files from the Avaya Support web site to your laptop.

Service packs may or may not be needed, depending on the release of Communication Manager and whether SES is optioned. For both new installations and upgrades, you may need to install a service pack after the installation.

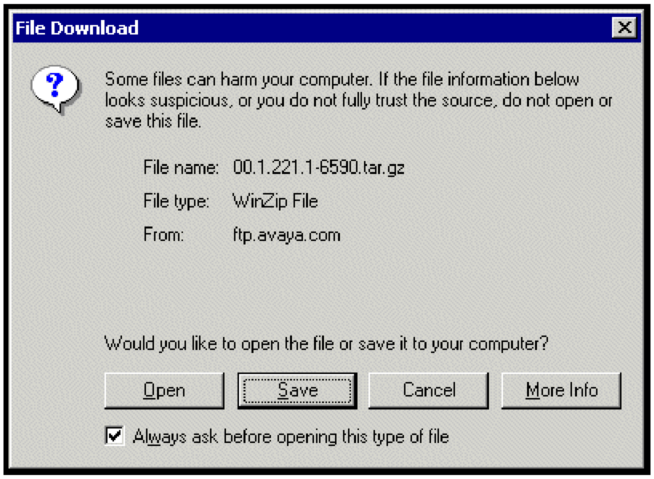
To download a service pack

1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access http://www.avaya.com/support on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At the Avaya support site, click **Downloads**
4. Click **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates**.
5. Scroll down to the **Software Update table for Servers running Communication Manager**.
6. Click the link for the appropriate G.A. load.
7. If you are a Business Partner, scroll to the bottom of the page and select **Download Center** to access the password protected Download Center. Otherwise, for Avaya, click **Latest**

Avaya Communication Manager x.x.x Service Pack to access the service pack download.

The File Download window appears.

File download window



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: 00.1.221.1-6590.tar.gz

File type: WinZip File

From: ftp.avaya.com

Would you like to open the file or save it to your computer?

⚠ **Important:**

While downloading the file it is possible that the Internet Explorer browser adds an extra character in the file name. Ensure that there are no extra characters in the file name before you save the file.

8. Click the **Save** button and browse to the directory on your laptop in which you want the file saved.

Obtaining service pack and language files for Communication Manager Messaging, if necessary

If Communication Manager Messaging will be installed, determine whether an service pack is needed and/or optional languages are used. If so, obtain the data files.

Obtaining an Communication Manager Messaging service pack file

If an Communication Manager Messaging service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an Communication Manager Messaging service pack file

1. On the Avaya Support Web site, click **Find Documentation and Downloads by Product Name**.
2. Under the letter "C", select **Communication Manager Messaging Application**.

3. Click **Downloads**.

   To download the Communication Manager Messaging patch software:

4. Click **Communication Manager Messaging Application Patches**.
5. Click the service pack file name for this release.

   For example, **C6072rf+b.rpm.**

6. Click **Save** and browse to the location on your laptop where you want to save the file.

   Note:

   The Communication Manager Messaging patch documentation is co-located with the patch software.

Obtaining optional language files

Optional languages are any language other than English (***us-eng*** or ***us-tdd)***. If optional languages are used with this Communication Manager Messaging, you must download the appropriate language files from a language CD after the upgrade. The customer should have the language CD(s) at the site. If not, you need to obtain the appropriate language CD(s) and take them to the site.

Obtaining Ethernet interface IP address and subnet mask

If Communication Manager Messaging is to be installed, you must obtain an IP address and subnet mask to be used for the Ethernet interface for the H.323 integration. The subnet mask must be the same as that used for the S8300 Server (control network), and is entered on the **Configure Server Web** screen when you configure the S8300.

Completing the RFA process (Obtaining license and authentication files)

Every S8300 Server and local survivable processor (LSP) requires a current and correct version of a license file in order to provide the expected call-processing service.

The Communication Manager license file specifies the features and services that are available on the S8300 Server, such as the number of ports purchased. The license file contains a software version number, hardware serial number, expiration date, and feature mask. The license file is reinstalled to add or remove call-processing features. New license files may be required when upgrade software is installed.

If the customer requires SES, you must acquire and install a separate SIP Enablement Services (SES) license file. You install the SES license as part of SES administrations, which you do after you install Communication Manager.

The Avaya authentication file contains the logins and passwords to access the S8300 Server. This file is updated regularly by Avaya services personnel, if the customer has a maintenance contract. All access to Communication Manager from any login is blocked unless a valid authentication file is present on the S8300 Server.

A new license file and the Avaya authentication file may be installed independently of each other or any other server upgrades.

Downloading license and password files

The license file for a S8300 configured as a Local Survivable Processor must have a feature set that is equal to or greater than the primary controller. A primary controller can be any of the following servers; S8300, S8400, S8500, S8700, S8710, S8720, or S8730 Server. This is necessary so that if control passes to the LSP, it can support the same level of call processing as that of the primary controller.

Additionally, the LSP must have a version of Communication Manager that is the same as, or later than, that of the primary controller.

Note:

The license file requirements of the LSP should be identified in your planning documentation.

To download the license and password files to your laptop

Tip:

Additional documentation on creating license files can be found on the RFA web site: http://rfa.avaya.com.

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and password files (for example, C:\licenses).
2. Visit the Remote Feature Activation web site, http://rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and password files for the customer.
4. Check that the license and password files are complete.

   You might need to add the serial number of the customer's media gateway.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and password files to your laptop.

Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary

This step is necessary only if the configuration of the customer’s INADS alarming modem has changed.

Note:

ART tool is available to Avaya associates and a few Business Partners. **Business Partners** who do not have access to the ART tool must call 800-295-0099.

The ART tool is a software tool that generates an IP address for a customer's INADS alarming modem. This IP address is required for configuring the S8300's modem for alarming.

Note:

You must generate a license and authentication file before you use the ART tool. Also, the ART process is available *only* to Avaya personnel. You need an ART login ID and password, which you can set up at the ART web site. Non-Avaya personnel must contact their service support or customer care center for INADS addresses, if required.

To run the ART

1. Access the ART web site on your laptop at http://ssdp.dr.avaya.com/vtac/jsp/portal.jsp.
2. Log in with SSO credential.
3. Click **Automatic Registration Tool** from My Tools list.
4. Select **Administer a Communication Manager (CM) product**.
   a. Enter the **RFA System ID** and **RFA Module ID**. The ID for system and module is generated using the RFA tool. If you do not have a system ID and module ID, visit the RFA tool and generate the IDs.
   b. Select **Installation Script Administration** as the session type.
   c. Select **S8300 Server** as the product type.
   d. Click **Start CM Product Administration**.

   A script file is created and downloaded or emailed to you.
5. You can use the installation script to set up an IP address and other alarming parameters automatically.

Obtaining the static *craft* password (Avaya technicians only)

After installing new software and a new Authentication file, you will need to use a static craft password to access the customer's system. This static password will enable you to log in to the S8300 with a direct connection to the Services port without the ASG challenge/response. To obtain the static password, call the ASG Conversant number, 800-248-1234 or 720-444-5557 and follow the prompts to get the password. In addition to your credentials, you will need to enter the customer's Product ID or the FL or IL number.

Business Partners must use the *dadmin* password after the installation. Call 877-295-0099 for more information.

Install the S8300

The following manual procedures cover:

- Inserting the S8300
- Installing Communication Manager Software

Inserting the S8300

You must connect a USB CD/DVD-ROM drive to the S8300 server *before* you completely seat the S8300 server in the slot. Use one of the following external USB CD/DVD-ROM drives:

There are three external CD/DVD-ROM drives that are supported on the S8300 Server:

- Avaya approved Panasonic Digistor 73082 or 73322 (Comcode: 700406267):
  - The switch must be turned to the ON position.
  - Instead of AC power, the Panasonic Digistor uses a Lithium ION battery for additional power. The CD/DVD-ROM draws more power than the USB port can supply. The additional power required is supplied by the Lithium ION battery. If the Lithium ION battery is depleted, a red LED displays and a failed to mount CD-ROM message appears. You can charge the Lithium ION battery by plugging the CD-ROM drive in a USB port for approximately 30 minutes. The Lithium ION battery charges faster if the ON/OFF switch is set to OFF.

  Note:

  The functionality of the Lithium ION battery supplying the extra power that the CD/DVD-ROM needs is only applicable for the original CD/DVD-ROM.
- Addonics (Model: AEPDVRWII824) (not available through Avaya):
  - Requires AC power to operate.
  - You must have the switch set to External.
- TEAC (end of sale) (Comcode: 700289580)

⚠ **CAUTION:**

Be sure to wear a properly grounded ESD wrist strap when handling the S8300 Server. Place all components on a grounded, static-free surface when working on them. When picking up the hard drive, be sure to hold it only on the edges.

To insert the S8300

1. Connect the USB DVD/CD-ROM drive to the S8300 as follows:

   a. Place the CD/DVD-ROM drive on a surface within 5 degrees of level.

b. If you are using an Addonics drive, plug one end of the CD/DVD-ROM power cord into the drive and plug the other end of the cord into an electrical outlet.

c. Set the power switch to **EXT** (Addonics drive) or to **ON** (Panasonic drive). The TEAC drive does not have a switch.

d. Connect the USB cable to one of the USB ports on the faceplate of the server and the other end of the USB cable to the CD/DVD-ROM drive.

2. Insert the Communication Manager Software CD-ROM into the external CD/DVD-ROM drive.

CAUTION:

Verify AC power connection to the laptop. Do not attempt to remaster the S8300 using only the laptop's battery power.

3. Push the S8300 module into the slot V1 guide until the front of the S8300 module aligns with the front faceplate of the gateway.

4. Secure the S8300 faceplate with the thumb screws.

   Tighten the thumb screws with a screw driver.

   Note:

   Unplug any external Compact Flash drive that might be connected to the S8300 USB ports. The S8300 tries to read any media connected to a USB port. The S8300 should only read the media on the CD-RW/DVD drive.

5. Power up the gateway by plugging in the power cord.

6. Connect the laptop to the Services port on the faceplate of the S8300.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See Laptop configuration for direct connection to the services port on page 31.

You will use SSH and the Maintenance Web Interface to perform the procedures. See the following:

- Accessing the server's command line interface with SSH on page 44
- Logging in to the S8300 Web Interface from your laptop on page 46

Note:

Communication Manager has telnet turned off by default. Therefore, telnet is not available after remastering of the hard drive is complete during an initial server installation. However, if the customer later chooses to enable telnet, you may be able to use telnet to access the server's command line interface.

See About connection and login methods on page 31 for details on how to physically connect and log into the S8300 Server.

Installing Communication Manager Software

Setting telnet parameters

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 interprets this as two key presses. You need to correct this before you telnet to the server.

Note:

This procedure is done entirely on your laptop, not on the S8300.

To set telnet parameters

1. Click **Start > Run** to open the Run dialog box.
2. Type **`telnet`** and press **Enter** to open a Microsoft Telnet session.
3. Type **`unset crlf`** and press **Enter**.
4. Type **`display`** and press **Enter** to confirm that either `Sending only CR` or `Line feed mode--causes the return key to send CR` displays.
5. Type quit or close the Telnet window by clicking on the **X** in the upper-right corner.

This resets your Microsoft Telnet defaults and does not need to be done each time you use Telnet.

installing the software

To do before you start the installation

1. Verify that the S8300 is inserted in slot V1.
2. Verify good AC power connections to the media gateway.
3. Avaya recommends using a UPS backup for S8300 Servers.

   If a UPS is present, make sure the media gateway is plugged into the UPS.

4. Verify that all Ethernet connections are secure, to ensure the file transfer process is not interrupted.

To install the software (Communication Manager and optionally, Communication Manager Messaging) on the server:

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter.**
3. If the DVD/CD drive was not attached to a USB port when the server booted up, you will not see any activity on the screen. In this case perform the following:

   a. Press the Shut Down button on the server.

   b. When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port.

   c. Unseat and reseat the S8300C in its slot.

   Tip:

   To navigate the installation 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.

4. Select **Install** and press **Enter**.

   The system displays the **Select Release Version** screen.

5. Select the appropriate release version then select **OK** and press **Enter**.

   The **Select Messaging Option** screen appears.

   Note:

   Communication Manager Messaging is optionally installed on the server when you install Communication Manager.

6. Select from one of the following:

   ● **CM Only <No Messaging>**

   ● **CMM <Embedded Messaging>**

   The following processes are initiated:

   - The server's hard drive and internal Compact Flash are partitioned and reformatted.
   - The Linux operating system is installed.
   - Once the drive is properly configured, Communication Manager software is installed, if you select CMM <Embedded Messaging> and the progress reported.

- If elected, Communication Manager Messaging is installed.

The process takes about 30 minutes. When the server is ready to reboot, the CD drive door opens or the CD is ejected, and a reminder to check the Avaya Support Site (support.avaya.com/downloads) for the latest software and firmware updates displays.

The reboot takes 1-3 minutes without Communication Manager Messaging and 3-6 minutes if it is present.

7. At your laptop click **Start > Run** to open the **Run** dialog box.
8. Type `ping -t 192.11.13.6` and press **Enter**.
9. Wait for the reply from the server to ensure connectivity to it.

Verifying Software Version

To verify the software version that you just installed:

1. Visit http://192.11.13.6.
2. On the Communication Manager Server Management Interface Web page, under the **Administration** menu, click **Server (Maintenance)**.
3. Select **Server > Software Version**.

   The **Software Version** page displays.
4. Verify that the server is running Release 5.2 software. The beginning of the **Report as:** string should show **R015x.02**.
5. Verify that the DVD/CD-ROM drive opened at the end of the software installation.
6. Disconnect the DVD/CD-ROM drive from the server's USB port.

Creating a super-user login

You must add a super-user account, also known as priveledged user account before you use Avaya Installation Wizard to configure the server and install the Avaya authentication file.

Note:

The passwords you administer for Communication Manager also apply to SES, if SES is optioned.

Note:

A craft level login can create a super-user login from Communication Manager release 4.0 or later.

To create a login:

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

   Note:

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

2. On the Communication Manager System Management Interface Web page, click **Server (Maintenance)** under the **Administration** menu.
3. Select **Security** > **Administrator Accounts**.

   The **Administrator Accounts** screen appears.

4. Select **Add Login**.
5. Select **Privileged Administrator** and click **Submit**.

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

6. Type a login name for the account in the **Login name** field.
7. Verify the following:
   - **susers** appears in the **Primary group** field.
   - **prof18** appears in the **Additional groups (profile)** field. *prof18* is the code for the customer super-user.
   - **/bin/bash** appears in the **Linux shell** field.
   - **/var/home/*login name*** appears in the **Home directory** field, where ***login name*** is the name you entered in step 6.
8. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
9. For the **Select type of authentication** option, select **password**.

   Note:

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

10. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
11. In the section **Force password/key change on next login** select **no**.
12. Click **Submit**.

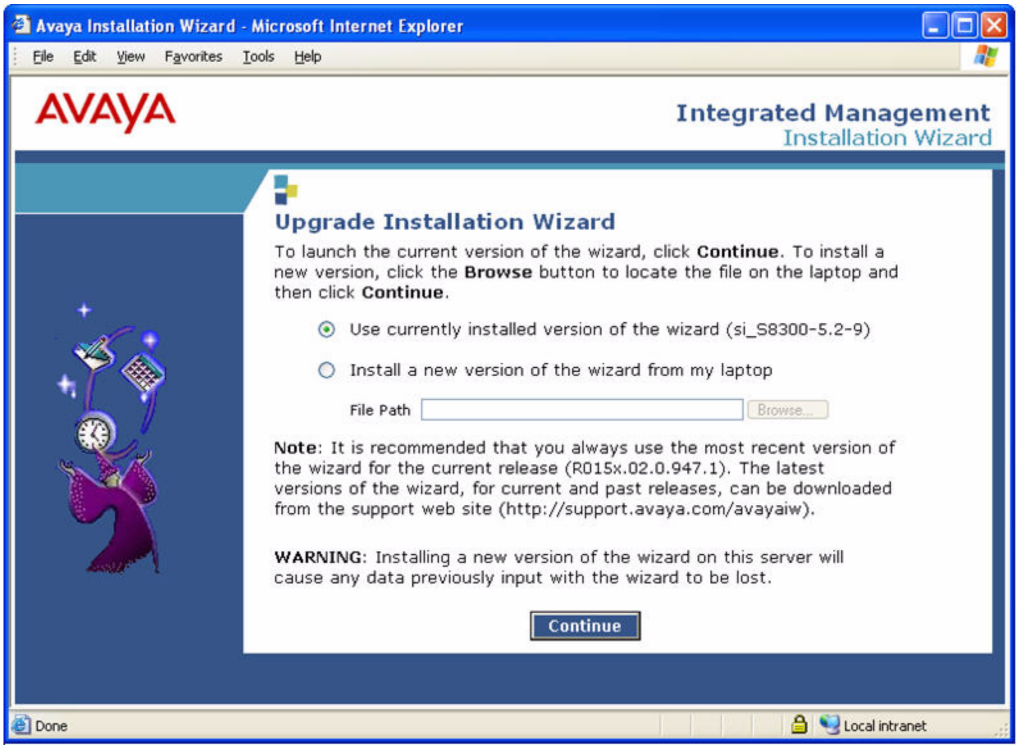
    The system informs you the login is added successfully.

Using the Avaya Installation Wizard (IW)

To configure the S8300 server using Avaya Installation Wizard:

1. Log in to the Communication Manager System Management Interface Web page.
2. Click **Avaya Installation Wizard** under the **Installation** menu. The **Upgrade Installation Wizard** screen appears.

Upgrade Installation Wizard screen


Avaya Installation Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
AVAYA
Integrated Management
Installation Wizard
Browse...
Continue
Done
Local intranet

Upgrade Installation Wizard

To launch the current version of the wizard, click **Continue**. To install a new version, click the **Browse** button to locate the file on the laptop and then click **Continue**.

● Use currently installed version of the wizard (si_S8300-5.2-9)

○ Install a new version of the wizard from my laptop

File Path

Note: It is recommended that you always use the most recent version of the wizard for the current release (R015x.02.0.947.1). The latest versions of the wizard, for current and past releases, can be downloaded from the support web site (http://support.avaya.com/avayaiw).

WARNING: Installing a new version of the wizard on this server will cause any data previously input with the wizard to be lost.

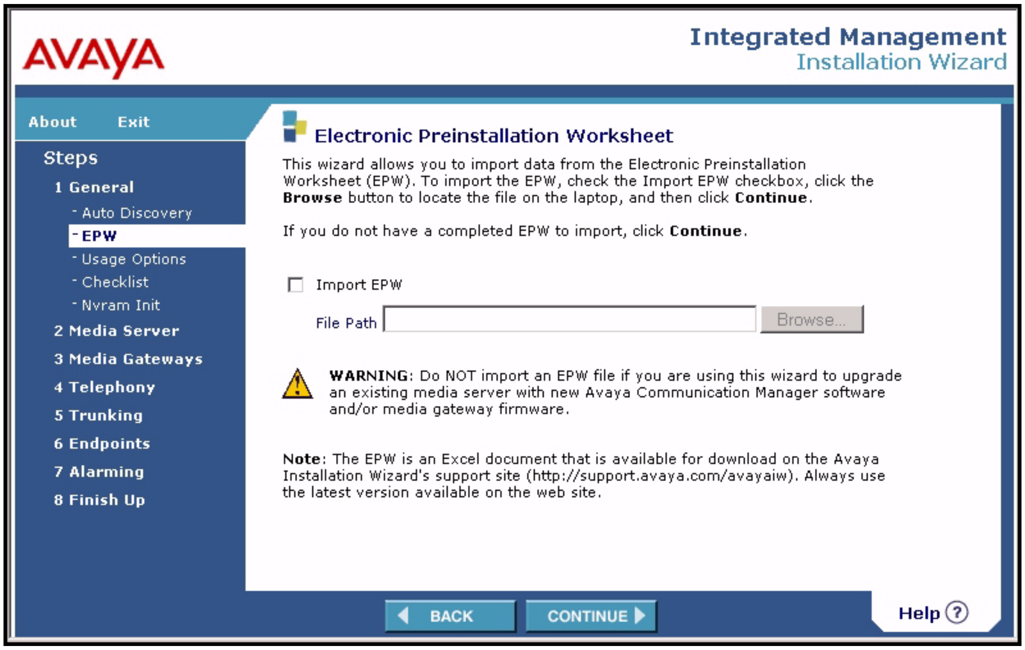
3. Select currently installed version of the Avaya Installation Wizard, or choose to install a new version of the Avaya Installation Wizard from your laptop, and click **Continue**.

   Brief **Overview** and **Auto Discovery** screens display system data for the installation, such as:

   - Server Type
   - Media Gateway Serial Number
   - Communication Manager Software Version

4. Click the **Continue** button, and the **Electronic Preinstallation Worksheet** screen appears.

Electronic Preinstallation Worksheet screen



Electronic Preinstallation Worksheet

This wizard allows you to import data from the Electronic Preinstallation Worksheet (EPW). To import the EPW, check the Import EPW checkbox, click the **Browse** button to locate the file on the laptop, and then click **Continue**.

If you do not have a completed EPW to import, click **Continue**.

□ Import EPW

File Path

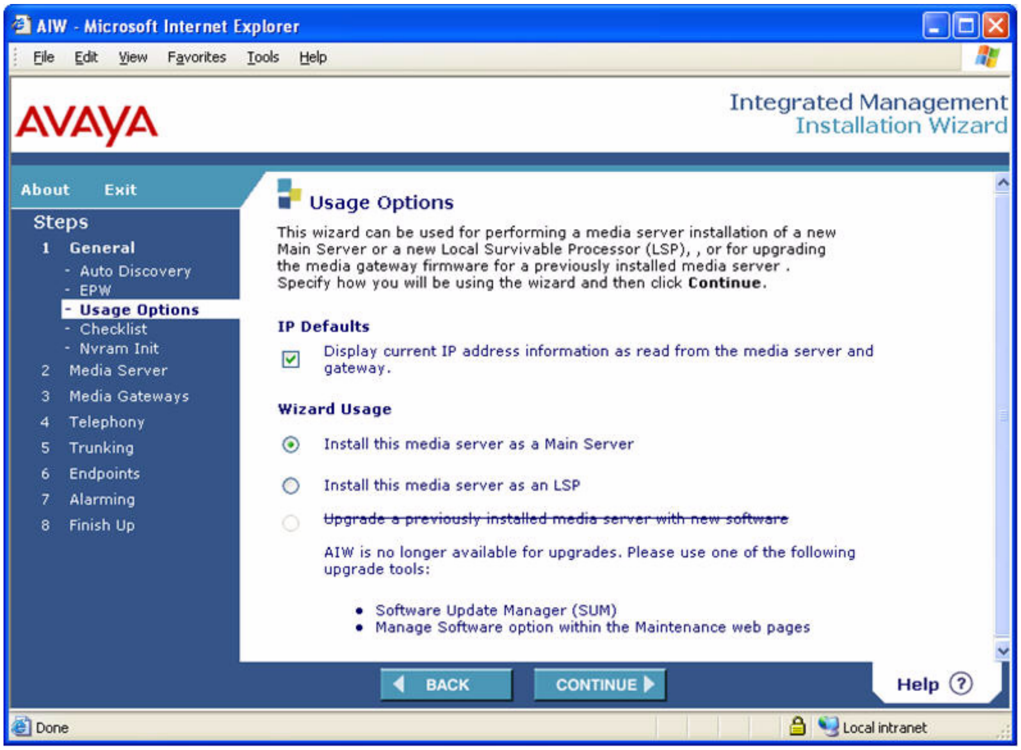
WARNING: Do NOT import an EPW file if you are using this wizard to upgrade an existing media server with new Avaya Communication Manager software and/or media gateway firmware.

Note: The EPW is an Excel document that is available for download on the Avaya Installation Wizard's support site (http://support.avaya.com/avayaiw). Always use the latest version available on the web site.

5. If you have an EPW loaded onto your laptop, select Import EPW and use the Browse button to locate the file on your laptop. If you do not have an EPW, you must later complete the fields on each page of the Avaya Installation Wizard using information from your project manager.

6. Click the **Continue** button. The **Usage Options** screen appears.

Usage Options screen



Steps
1 General
- Auto Discovery
- EPW
- Usage Options
- Checklist
- Nvram Init
2 Media Server
3 Media Gateways
4 Telephony
5 Trunking
6 Endpoints
7 Alarming
8 Finish Up

Usage Options

This wizard can be used for performing a media server installation of a new Main Server or a new Local Survivable Processor (LSP), , or for upgrading the media gateway firmware for a previously installed media server . Specify how you will be using the wizard and then click **Continue**.

IP Defaults

☑ Display current IP address information as read from the media server and gateway.

Wizard Usage

● Install this media server as a Main Server

○ Install this media server as an LSP

○ ~~Upgrade a previously installed media server with new software~~

AIW is no longer available for upgrades. Please use one of the following upgrade tools:

- Software Update Manager (SUM)
- Manage Software option within the Maintenance web pages

7. Select either **Install this media server as a Main server** or **Install this media server as an LSP**. Leave the **IP Defaults** checkbox unchecked.

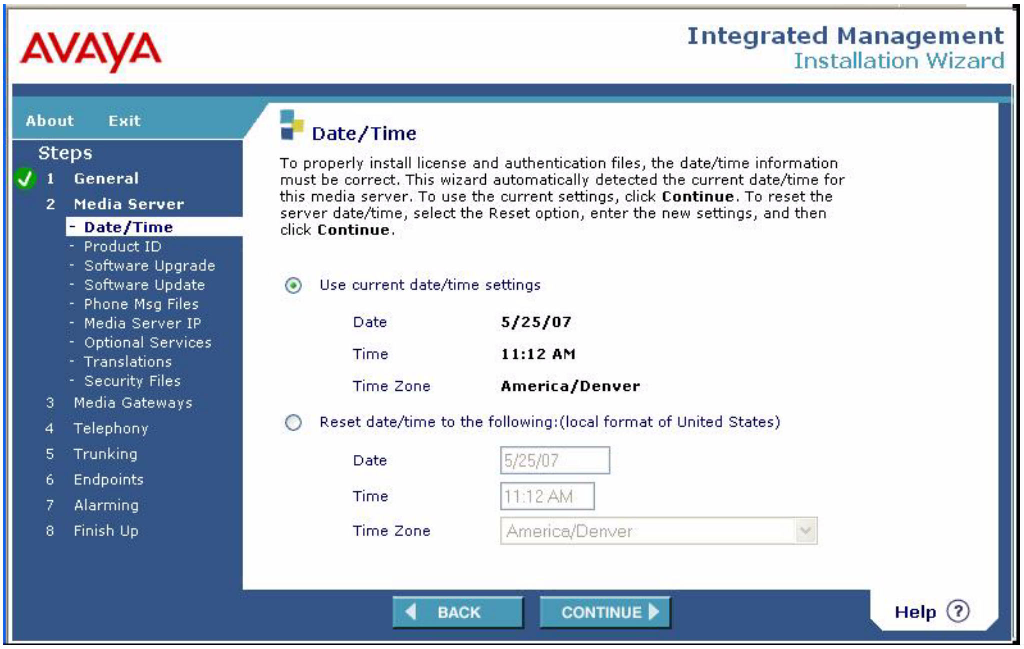
8. Click **Continue**, after which you will be asked to confirm your choice of Wizard Usage before continuing.

   After reviewing a checklist of required and optional items for continuing the installation, you then have the option to run the `nvram initialize` command, which restores all factory default settings on all available media gateways. For a new installation, this is unnecessary.

9. Click **Continue** to begin the **Server** tasks.

   The **Date/Time** screen appears.

Date/Time screen



Date/Time

To properly install license and authentication files, the date/time information must be correct. This wizard automatically detected the current date/time for this media server. To use the current settings, click **Continue**. To reset the server date/time, select the Reset option, enter the new settings, and then click **Continue**.

● Use current date/time settings

Date	**5/25/07**
Time	**11:12 AM**
Time Zone	**America/Denver**

○ Reset date/time to the following:(local format of United States)

Date	5/25/07
Time	11:12 AM
Time Zone	America/Denver

10. Choose the current date and time information that the Avaya Installation Wizard detects on the S8300. If necessary, you can reset the date, time, and time zone. If you set the server time, make sure to set it to within five (5) minutes of the Network Timer Server (NTS) time, date and time zone so that synchronization can occur.

    Note:

    If you are configuring an LSP, the date and time must match the time zone of the primary controller.

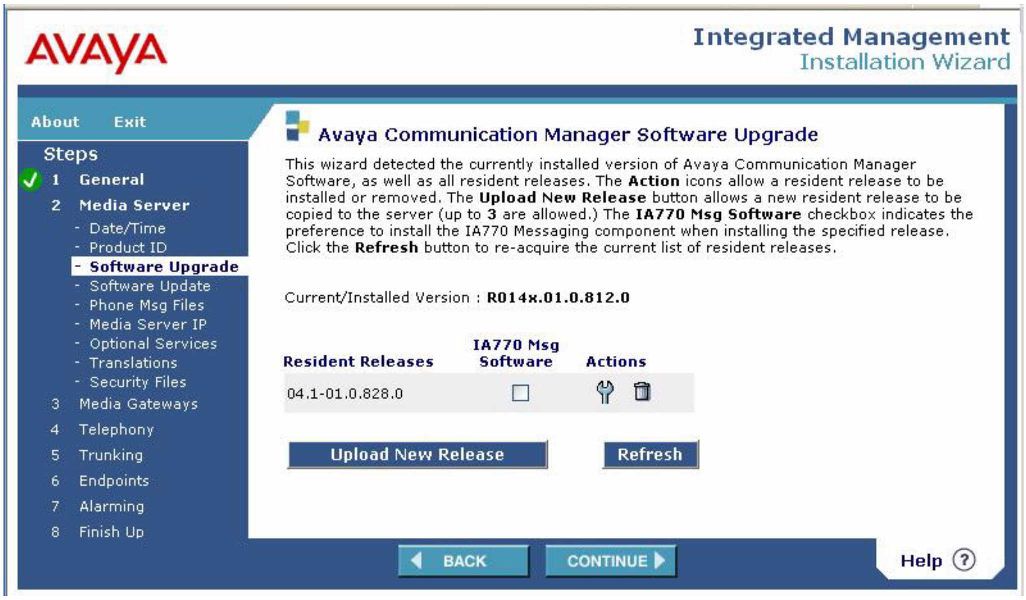
11. Click **Continue**.

    The Avaya Installation Wizard displays the **Product ID** screen, which Avaya installers use. The screen is not used by business partners.

12. Enter the product ID you obtained through the ART tool, and click **Continue**.

    The **Avaya Communication Manager Software Upgrade** screen displays the version of Communication Manager you just installed.

Avaya Communication Manager Software Upgrade screen



Avaya Communication Manager Software Upgrade

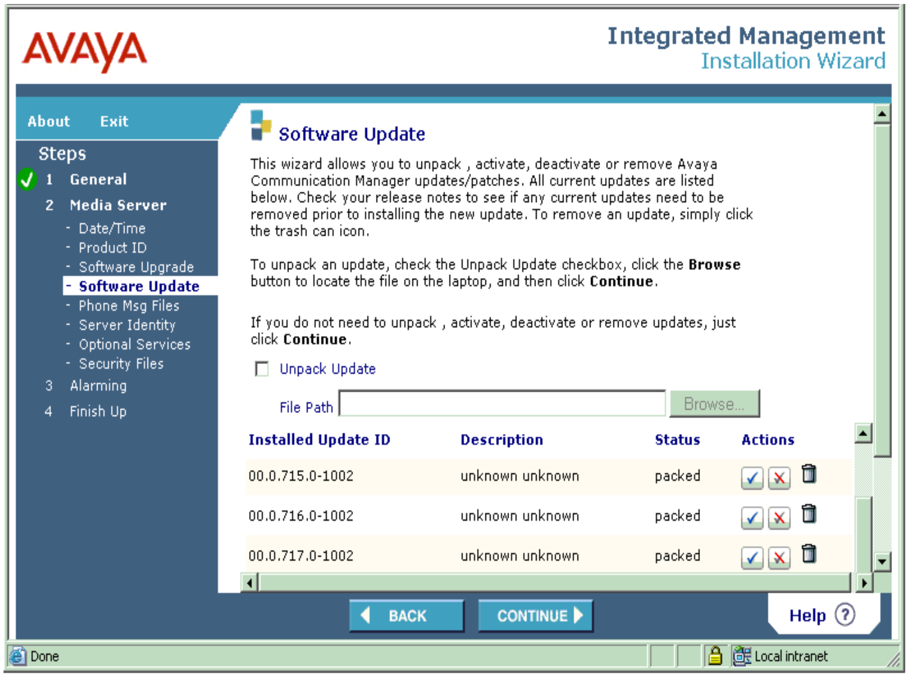
This wizard detected the currently installed version of Avaya Communication Manager Software, as well as all resident releases. The **Action** icons allow a resident release to be installed or removed. The **Upload New Release** button allows a new resident release to be copied to the server (up to **3** are allowed.) The **IA770 Msg Software** checkbox indicates the preference to install the IA770 Messaging component when installing the specified release. Click the **Refresh** button to re-acquire the current list of resident releases.

Current/Installed Version : **R014x.01.0.812.0**

Resident Releases	IA770 Msg Software	Actions
04.1-01.0.828.0	□	🗑

13. Click **Continue.**

The **Software Update** screen appears.



Software Update

This wizard allows you to unpack , activate, deactivate or remove Avaya Communication Manager updates/patches. All current updates are listed below. Check your release notes to see if any current updates need to be removed prior to installing the new update. To remove an update, simply click the trash can icon.

To unpack an update, check the Unpack Update checkbox, click the **Browse** button to locate the file on the laptop, and then click **Continue**.

If you do not need to unpack , activate, deactivate or remove updates, just click **Continue**.

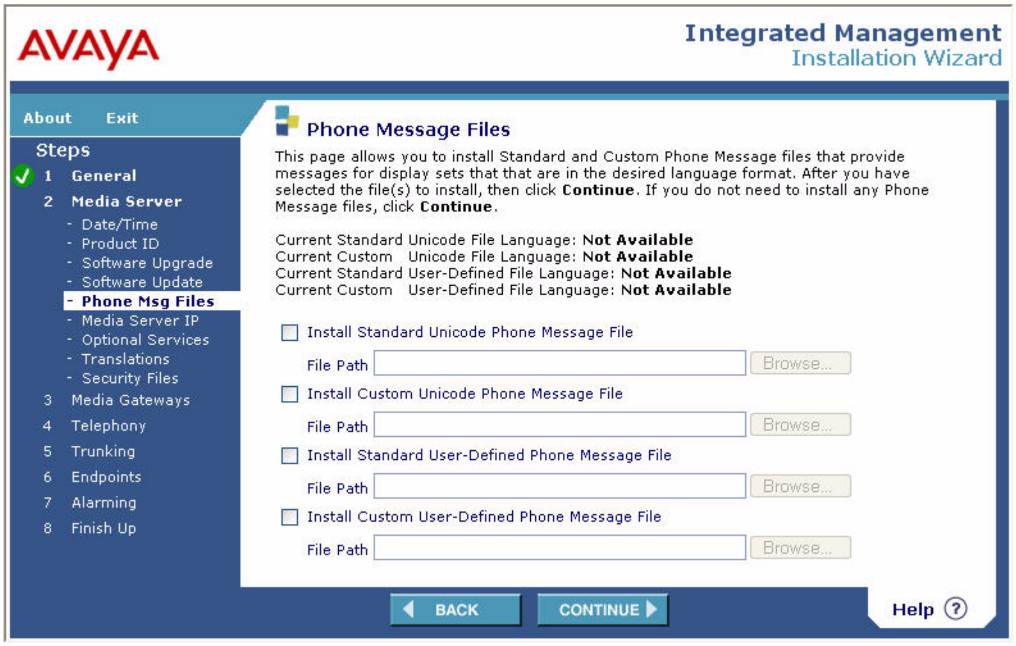
□ Unpack Update

File Path

Installed Update ID	Description	Status	Actions
00.0.715.0-1002	unknown unknown	packed	✓ ✗ 🗑
00.0.716.0-1002	unknown unknown	packed	✓ ✗ 🗑
00.0.717.0-1002	unknown unknown	packed	✓ ✗ 🗑

14. Do one or both of the following:
    - If there is an update or security file you need to download, click the **Browse** button to locate the file.
    - If the file you need to install needs to be unpacked, click the **Unpack** box.
15. Select the file you want to activate and click **Activate**.
16. Click **Continue**.

    The **Phone Message Files** screen appears. This screen allows you to install standard and custom phone message files that provide messages for display sets that are in the desired language format.



Phone Message Files

This page allows you to install Standard and Custom Phone Message files that provide messages for display sets that that are in the desired language format. After you have selected the file(s) to install, then click **Continue**. If you do not need to install any Phone Message files, click **Continue**.

Current Standard Unicode File Language: **Not Available**
Current Custom Unicode File Language: **Not Available**
Current Standard User-Defined File Language: **Not Available**
Current Custom User-Defined File Language: **Not Available**

☐ Install Standard Unicode Phone Message File

File Path [ ] Browse...

☐ Install Custom Unicode Phone Message File

File Path [ ] Browse...

☐ Install Standard User-Defined Phone Message File

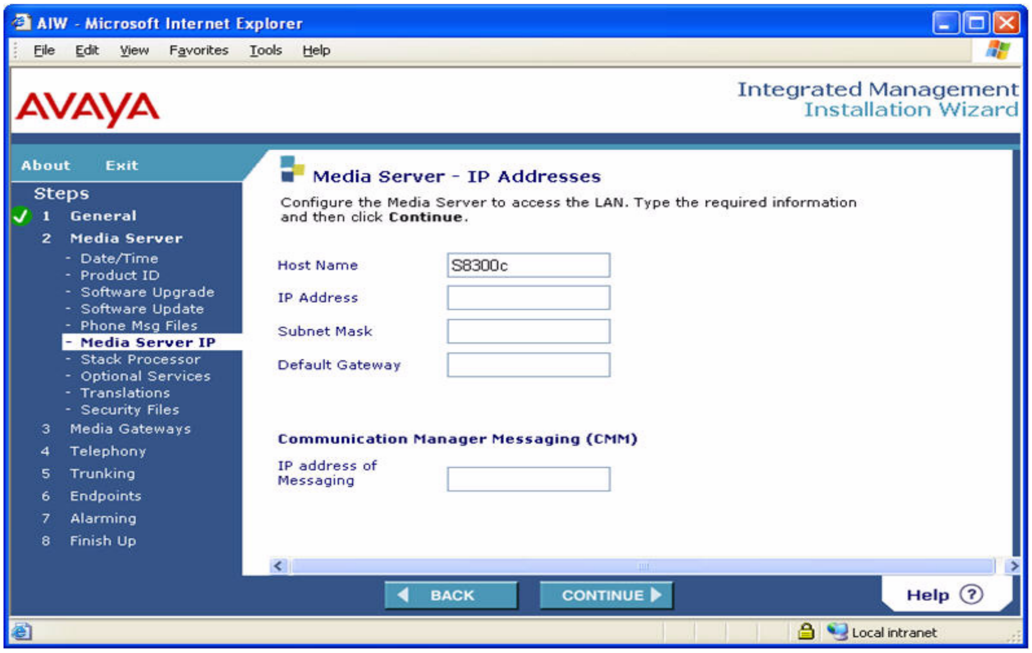
File Path [ ] Browse...

☐ Install Custom User-Defined Phone Message File

File Path [ ] Browse...

17. Click **Continue**.

    The **Media Server - IP Addresses** screen appears.



Media Server - IP Addresses

Configure the Media Server to access the LAN. Type the required information and then click **Continue**.

Host Name: S8300c

IP Address:

Subnet Mask:

Default Gateway:

Communication Manager Messaging (CMM)

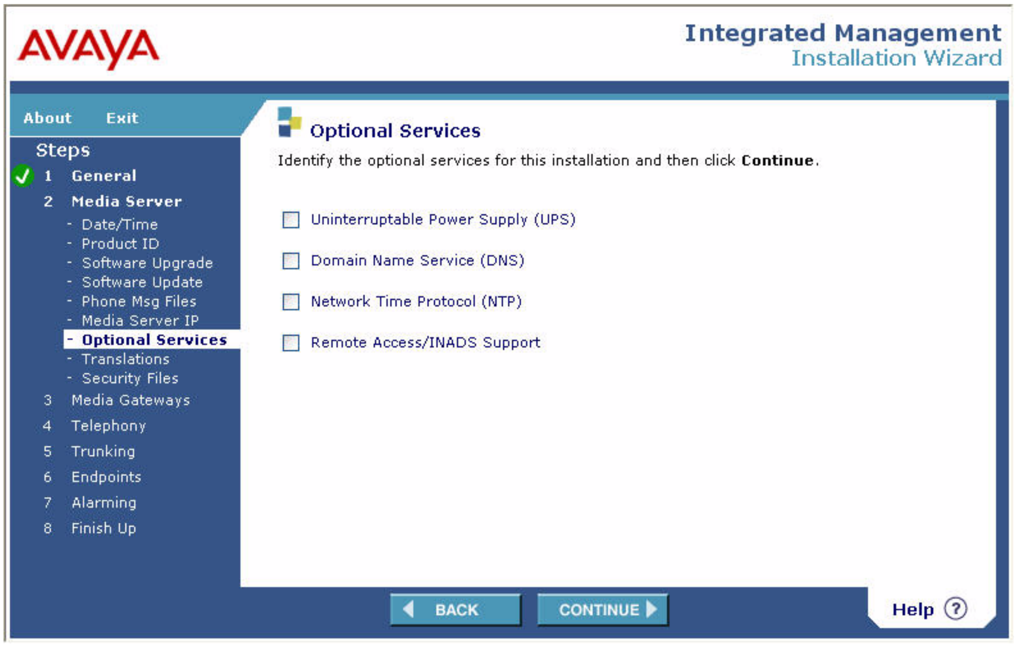
IP address of Messaging:

18. Enter the required information. If your S8300 Server is already configured, the Avaya Installation Wizard should detect and display its address information in this screen.

19. Click **Continue**.

    If you selected one of the wizard usage options for configuring an LSP in the **Usage Options** screen, the **Primary Controller IP Address** screen appears. The IP address fields differ depending on the type of primary controller. Enter the required IP address(es) for the primary controller.

20. The **Optional Services** screen appears. Select the services you want.



Optional Services

Identify the optional services for this installation and then click **Continue**.

□ Uninterruptable Power Supply (UPS)

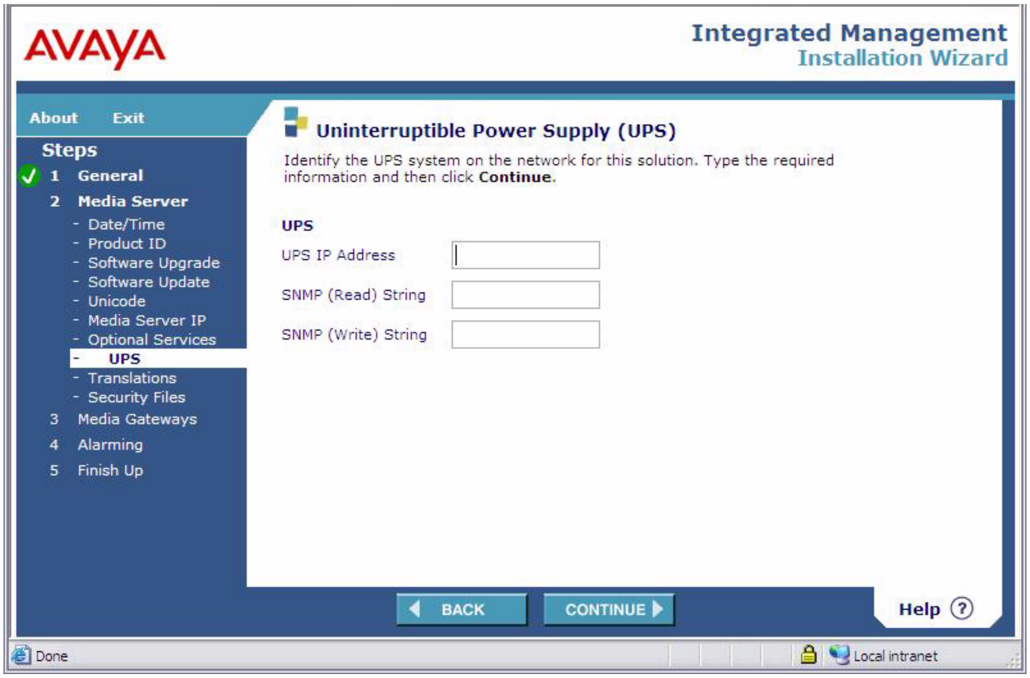
□ Domain Name Service (DNS)

□ Network Time Protocol (NTP)

□ Remote Access/INADS Support

21. Click **Continue**.

If you selected Uninterruptible Power Supply (UPS) in the **Optional Services** screen, the **Uninterruptible Power Supply (UPS)** screen appears. Enter the required information.



Uninterruptible Power Supply (UPS)

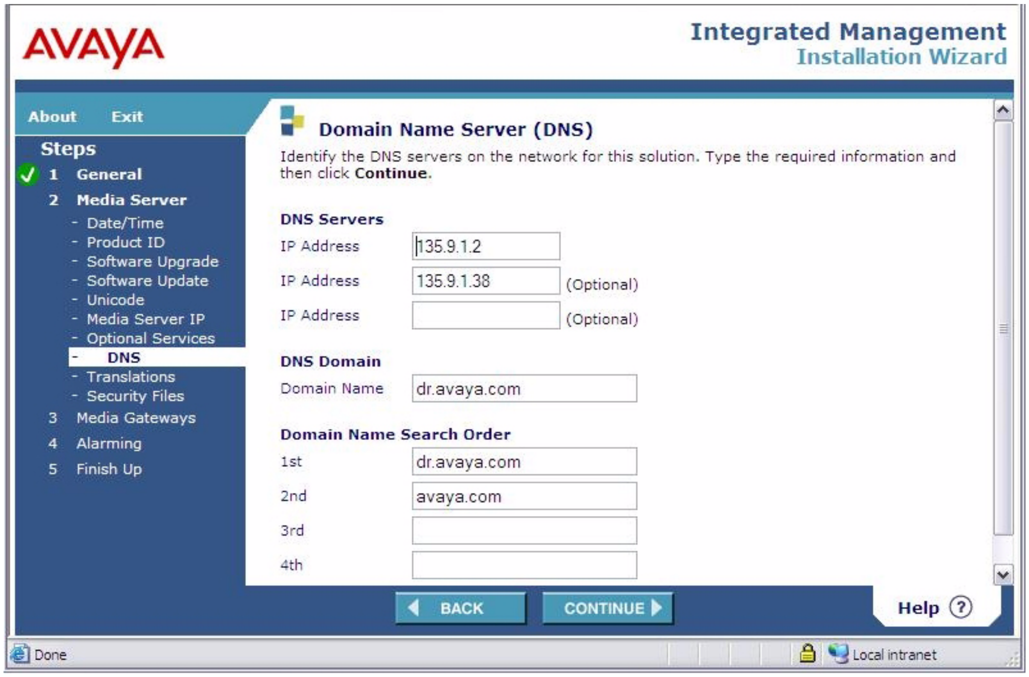
Identify the UPS system on the network for this solution. Type the required information and then click **Continue**.

UPS

UPS IP Address	
SNMP (Read) String	
SNMP (Write) String	

22. Click **Continue**.

    If you selected Domain Name Service (DNS) in the **Optional Services** screen, the **Domain Name Service (DNS)** screen appears. Enter the required information.



Domain Name Server (DNS)

Identify the DNS servers on the network for this solution. Type the required information and then click **Continue**.

DNS Servers

IP Address 135.9.1.2

IP Address 135.9.1.38 (Optional)

IP Address (Optional)

DNS Domain

Domain Name dr.avaya.com

Domain Name Search Order

1st dr.avaya.com

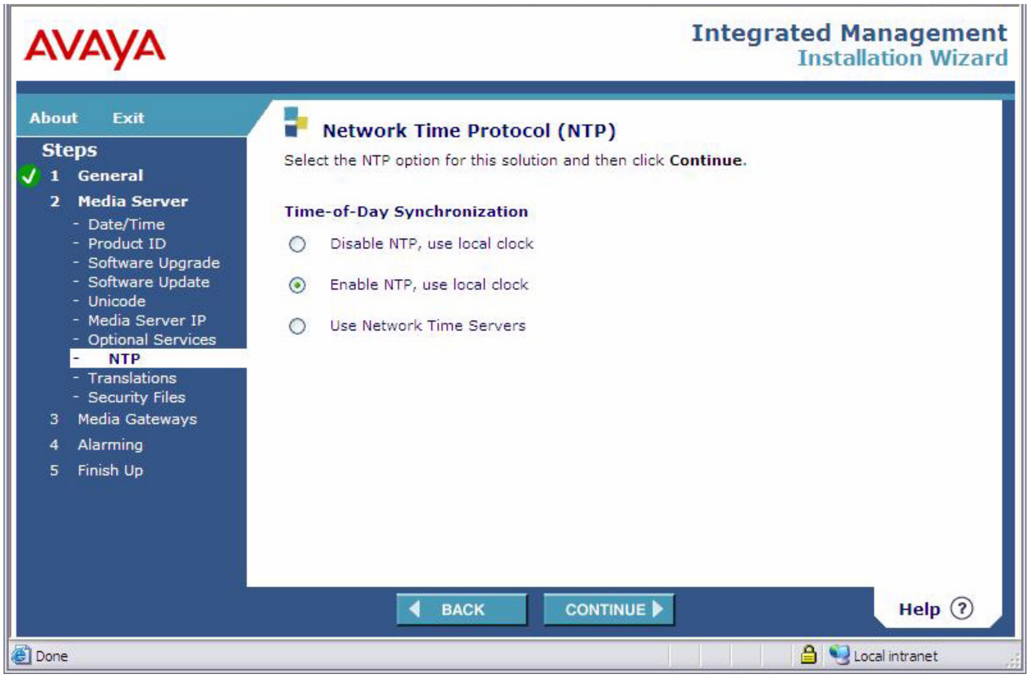
2nd avaya.com

3rd

4th

23. Click **Continue**.

    If you selected Network Time Protocol (NTP) in the **Optional Services** screen, the **Network Time Protocol (NTP)** screen appears. Select an NTP option.



Network Time Protocol (NTP)

Select the NTP option for this solution and then click **Continue**.

Time-of-Day Synchronization

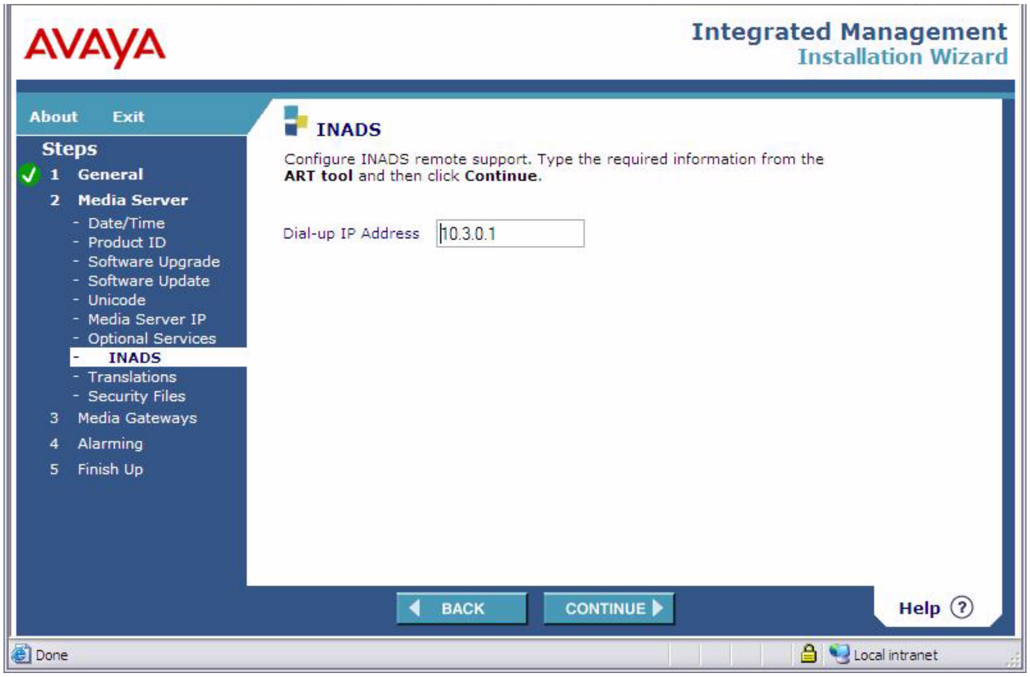
○ Disable NTP, use local clock

● Enable NTP, use local clock

○ Use Network Time Servers

24. Click **Continue**.

    If you selected Remote Access/INADS Support in the **Optional Services** screen, the **INADS** screen appears. Enter a dialup IP address for Installation and Administration System (INADS) remote support.



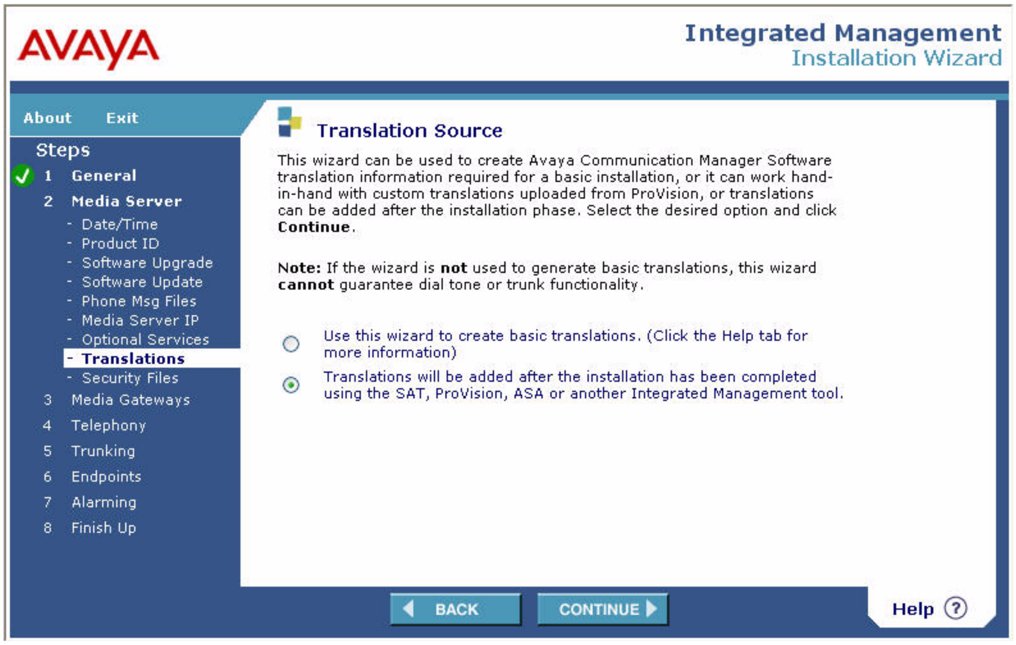
INADS

Configure INADS remote support. Type the required information from the **ART tool** and then click **Continue**.

Dial-up IP Address: 10.3.0.1

25. Click **Continue**.

    The **Translation Source** screen appears if this server is a primary controller. This screen allows you to generate Communication Manager translation information. This feature provides basic translations for administration of extension ranges, trunk types, routes, class of service, feature access codes, trunk access codes, station button assignment, and several other parameters.



Translation Source

This wizard can be used to create Avaya Communication Manager Software translation information required for a basic installation, or it can work hand-in-hand with custom translations uploaded from ProVision, or translations can be added after the installation phase. Select the desired option and click **Continue**.

Note: If the wizard is **not** used to generate basic translations, this wizard **cannot** guarantee dial tone or trunk functionality.

○ Use this wizard to create basic translations. (Click the Help tab for more information)

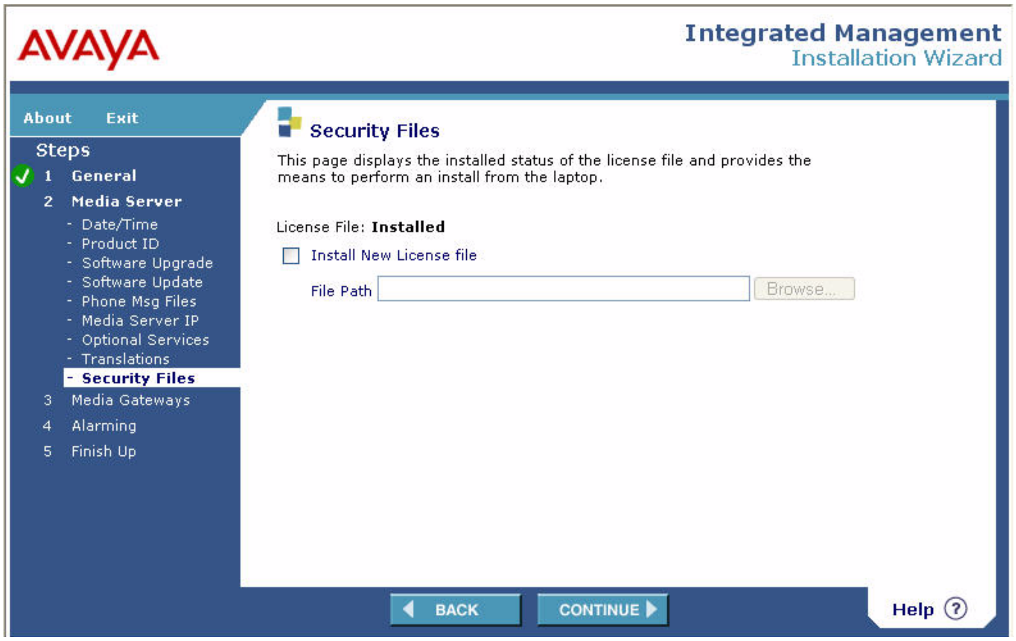
● Translations will be added after the installation has been completed using the SAT, ProVision, ASA or another Integrated Management tool.

26. Click **Continue**.

    The **Security Files** screen appears. This screen displays the status of your Communication Manager license file, and allows you to install this file from a laptop.

Note:

If you selected **Use this wizard to create basic translations** in the **Translation Source** screen, the **Security Files** screen displays also the installed status of the CM's authentication file and enables you to install or replace the authentication file from the laptop or LAN source.



Security Files

This page displays the installed status of the license file and provides the means to perform an install from the laptop.

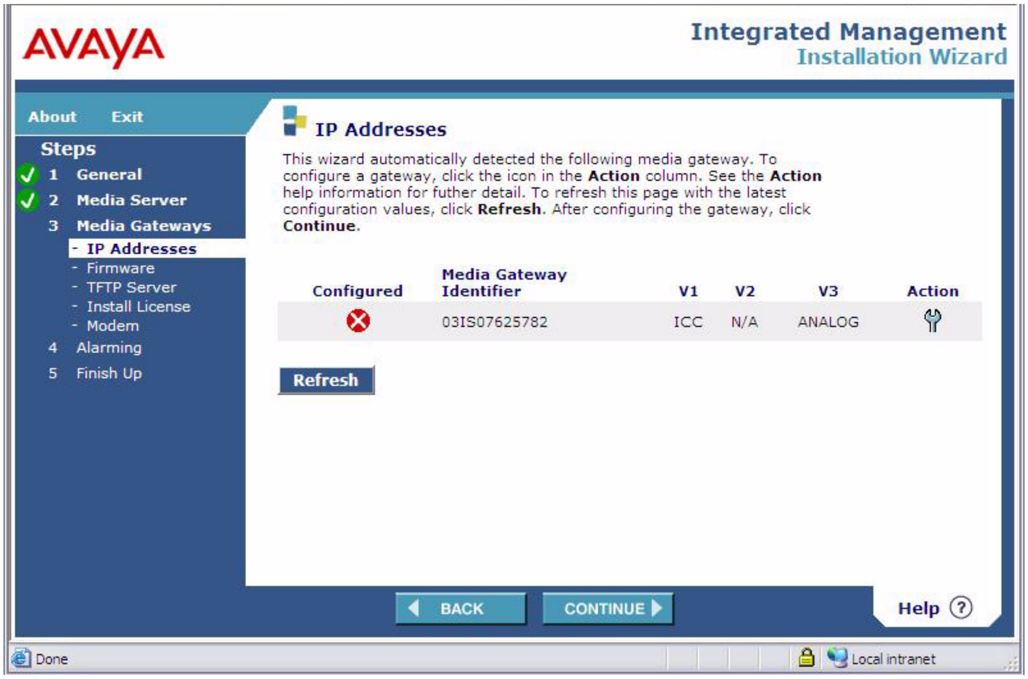
License File: **Installed**

□ Install New License file

File Path

27. Click **Continue**.

    The **IP Addresses** screen appears. This screen displays the ID of the media gateway, as well as the type of media module residing in each slot of the media gateway's chassis.



IP Addresses

This wizard automatically detected the following media gateway. To configure a gateway, click the icon in the **Action** column. See the **Action** help information for futher detail. To refresh this page with the latest configuration values, click **Refresh**. After configuring the gateway, click **Continue**.

Configured	Media Gateway Identifier	V1	V2	V3	Action
✗	031S07625782	ICC	N/A	ANALOG	🔧

28. To continue, click the 🔧 icon corresponding to the media gateway in the **Action** column.

29. Enter the following information in the IP Address - Media Gateway screen:

    - **IP Address** — the IP address assigned to the Media Gateway Processor
    - **Subnet Mask** — the subnet mask assigned to the Media Gateway Processor
    - **VLAN Number** — the VLAN assigned to the Media Gateway Processor, normally the same VLAN assigned to the primary controller

30. Click **Continue**.

31. Complete the fields as follows for each IP Route number on the **Static Route** screen:

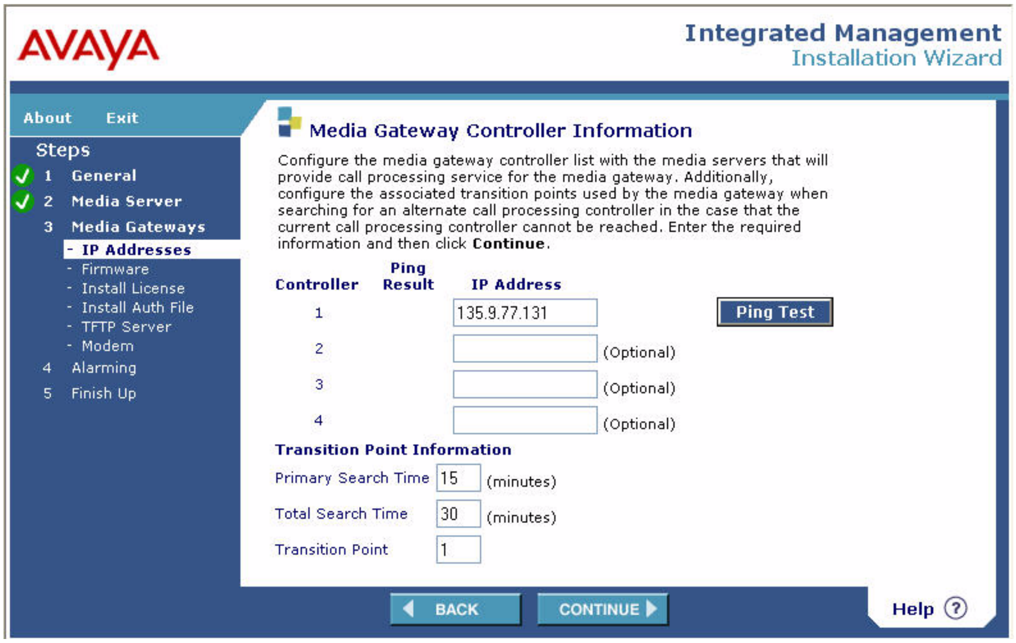
    - **Destination IP Address** — the default 0.0.0.0 or the IP address of the destination IP route
    - **Destination Subnet Mask** — the default 0.0.0.0 or the subnet mask of the destination IP route
    - **Gateway IP Address** — the IP address of the default network gateway for the route

    ⚠ **CAUTION:**

    The default gateway IP address is required for Communication Manager 5.2.

32. Click **Continue**.

    The **Media Gateway Controller Information** screen appears. Configure the list of Media Gateway Controllers (MGCs) that provides call processing services for the media gateways. You must specify a primary MGC in the first IP address box. You can specify up to three backup MGCs in the optional IP address boxes, in priority order. The media gateway searches for the primary MGC first. If it cannot connect to the primary MGC, it searches for a backup MGC. S8300, S8400, S8500, S8700-Series Servers support Processor Ethernet. So the MGC can be a Primary Controller, C-LAN, LSP, or ESS. Specify your primary MGC in accordance with the usage option you chose. If you do not configure the S8300 installed in the media gateway as the primary MGC, configure the S8300 as a backup MGC.



Media Gateway Controller Information

Configure the media gateway controller list with the media servers that will provide call processing service for the media gateway. Additionally, configure the associated transition points used by the media gateway when searching for an alternate call processing controller in the case that the current call processing controller cannot be reached. Enter the required information and then click **Continue**.

Controller	Ping Result	IP Address	
1		135.9.77.131	
2			(Optional)
3			(Optional)
4			(Optional)

Transition Point Information

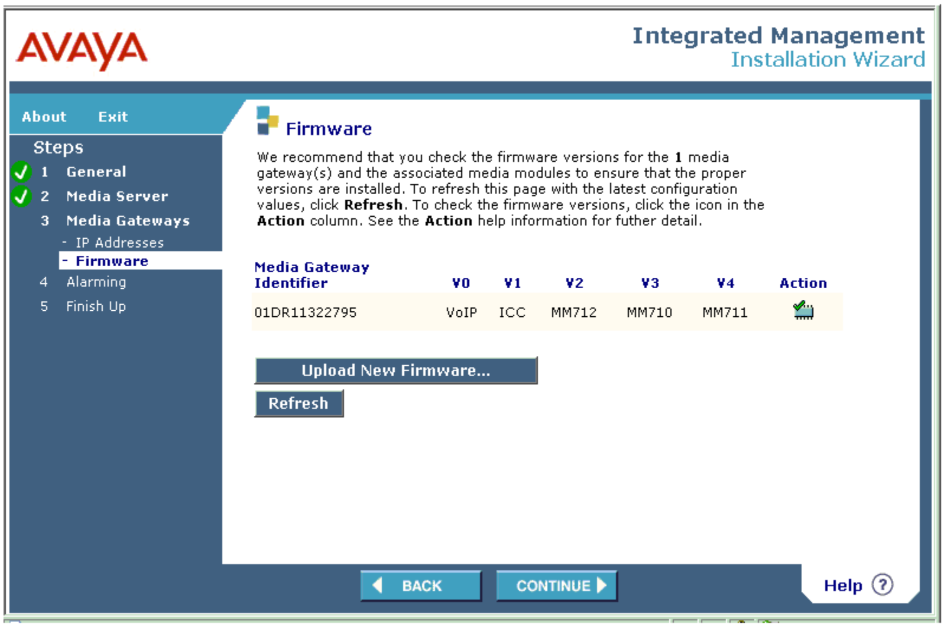
Primary Search Time 15 (minutes)

Total Search Time 30 (minutes)

Transition Point 1

33. To upgrade the firmware on the media gateway, click **Continue** on the **Media Gateway Controller Information** screen.

    The **Firmware** screen appears.



Firmware

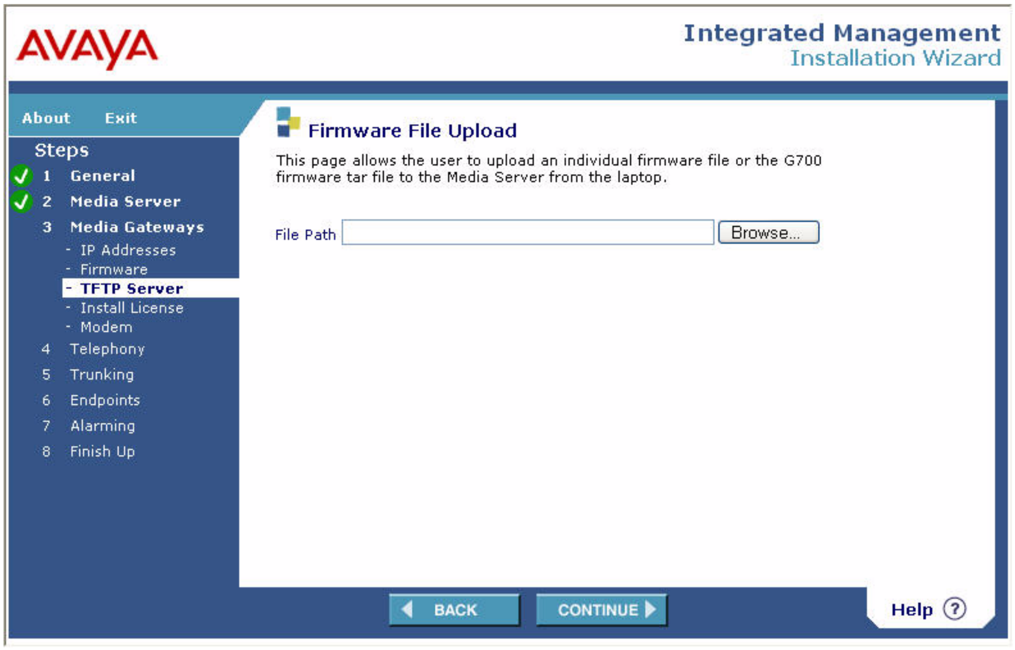
We recommend that you check the firmware versions for the **1** media gateway(s) and the associated media modules to ensure that the proper versions are installed. To refresh this page with the latest configuration values, click **Refresh**. To check the firmware versions, click the icon in the **Action** column. See the **Action** help information for futher detail.

Media Gateway Identifier	V0	V1	V2	V3	V4	Action
01DR11322795	VoIP	ICC	MM712	MM710	MM711	✓

34. Click **Upload New Firmware**.

    The **Firmware File Upload** screen appears. This screen allows you to upload a new firmware file from a laptop.

35. Click **Browse** to select the path of the file you want to upload.



Firmware File Upload

This page allows the user to upload an individual firmware file or the G700 firmware tar file to the Media Server from the laptop.

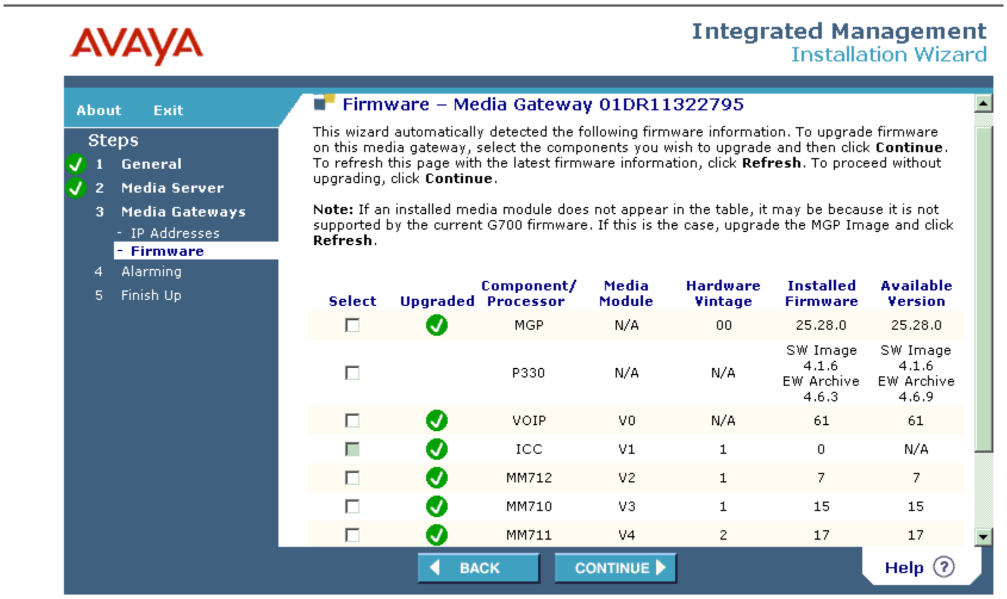
File Path [ ] Browse...

36. Click **Continue** to upload the file.

    The **Firmware** screen appears.

37. To upgrade firmware, select the action icon.

    This screen displays the currently installed firmware versions on the media gateway and its media modules, as well as the most recent available versions.



Firmware – Media Gateway 01DR11322795

This wizard automatically detected the following firmware information. To upgrade firmware on this media gateway, select the components you wish to upgrade and then click **Continue**. To refresh this page with the latest firmware information, click **Refresh**. To proceed without upgrading, click **Continue**.

Note: If an installed media module does not appear in the table, it may be because it is not supported by the current G700 firmware. If this is the case, upgrade the MGP Image and click **Refresh**.

Select	Upgraded	Component/ Processor	Media Module	Hardware Vintage	Installed Firmware	Available Version
□	✓	MGP	N/A	00	25.28.0	25.28.0
□		P330	N/A	N/A	SW Image 4.1.6 EW Archive 4.6.3	SW Image 4.1.6 EW Archive 4.6.9
□	✓	VOIP	V0	N/A	61	61
□	✓	ICC	V1	1	0	N/A
□	✓	MM712	V2	1	7	7
□	✓	MM710	V3	1	15	15
□	✓	MM711	V4	2	17	17

38. Select the modules you want to upgrade and click **Continue**.
39. To proceed without upgrading any firmware, clear all the boxes in the **Select** column and click **Continue**.

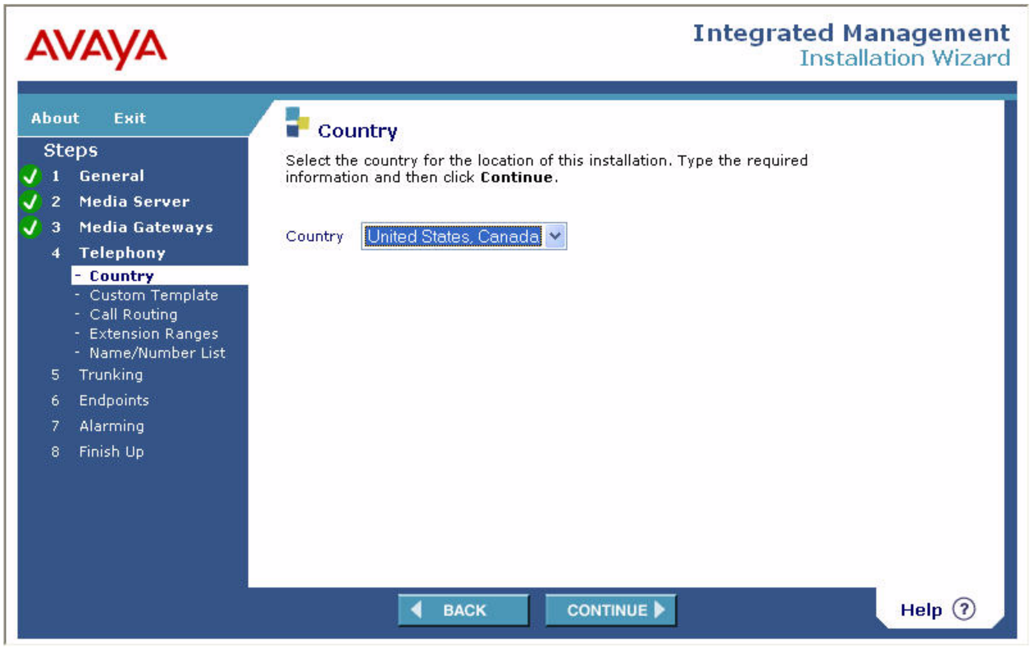
    If you are adding translations using the wizard, the **Country** screen appears. Go to Telephony configuration on page 143.

    If you are not adding translations using the wizard, the **Modem Status** screen appears. Go to Alarm configuration on page 156.

Telephony configuration

To configure translations, do the following:

1. On the **Country** screen, select the country in which the installation is taking place**.**



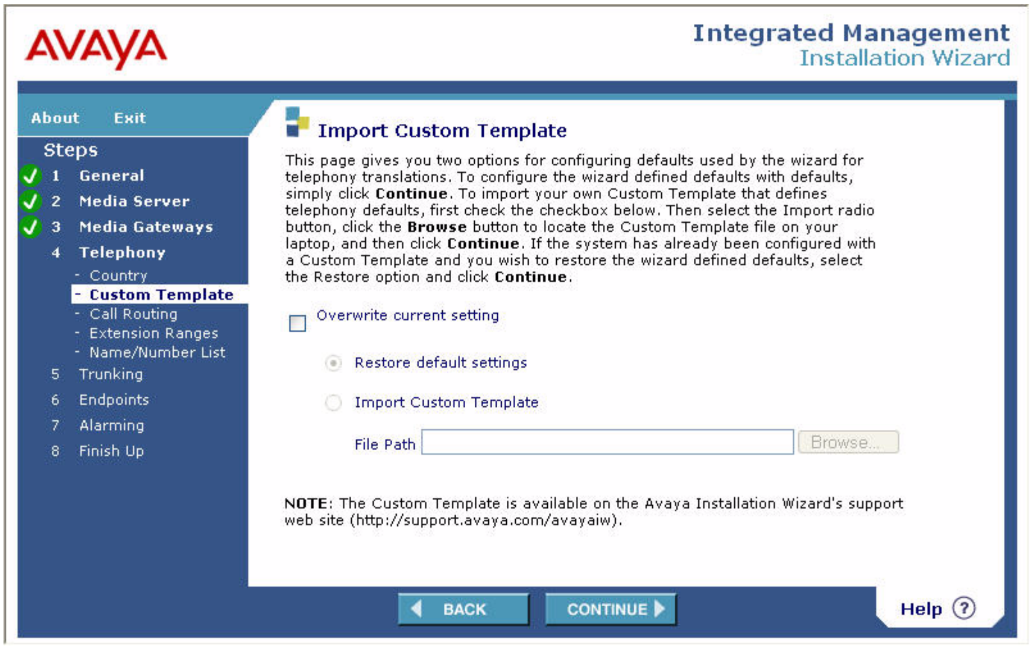
Country

Select the country for the location of this installation. Type the required information and then click **Continue**.

Country: United States, Canada

2. Click **Continue**.

   The **Import Custom Template** screen appears. This screen enables you to configure telephony translation defaults for the Avaya IW.



Import Custom Template

This page gives you two options for configuring defaults used by the wizard for telephony translations. To configure the wizard defined defaults with defaults, simply click **Continue**. To import your own Custom Template that defines telephony defaults, first check the checkbox below. Then select the Import radio button, click the **Browse** button to locate the Custom Template file on your laptop, and then click **Continue**. If the system has already been configured with a Custom Template and you wish to restore the wizard defined defaults, select the Restore option and click **Continue**.

□ Overwrite current setting

● Restore default settings

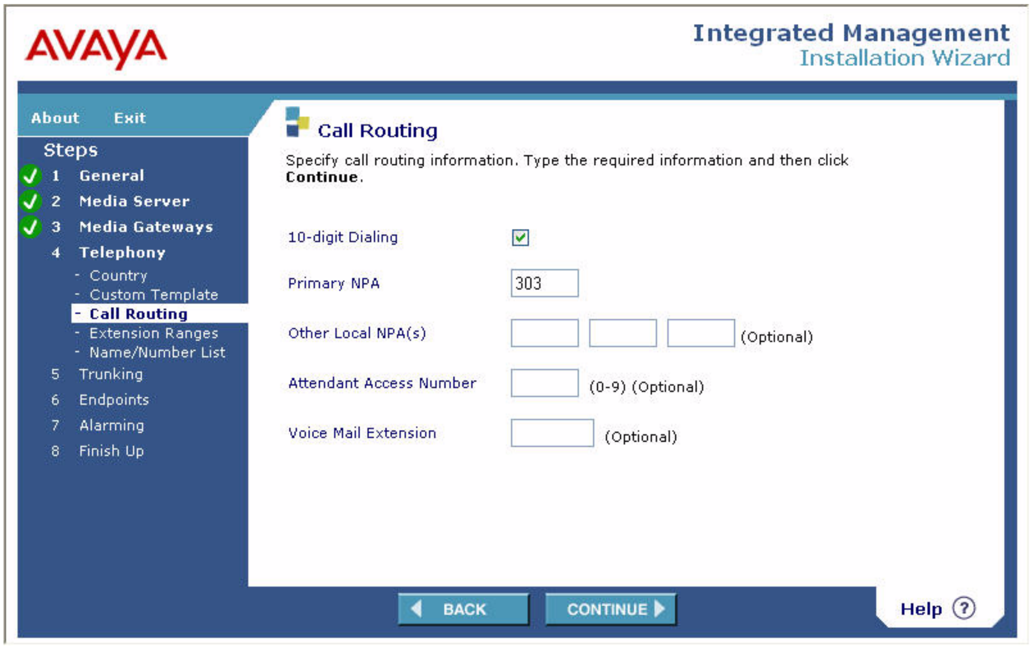
○ Import Custom Template

File Path [   ] Browse...

NOTE: The Custom Template is available on the Avaya Installation Wizard's support web site (http://support.avaya.com/avayaiw).

3. Click **Continue**.

   The **Call Routing** screen appears. Enter the required call routing information.



Call Routing

Specify call routing information. Type the required information and then click **Continue**.

10-digit Dialing ☑

Primary NPA 303

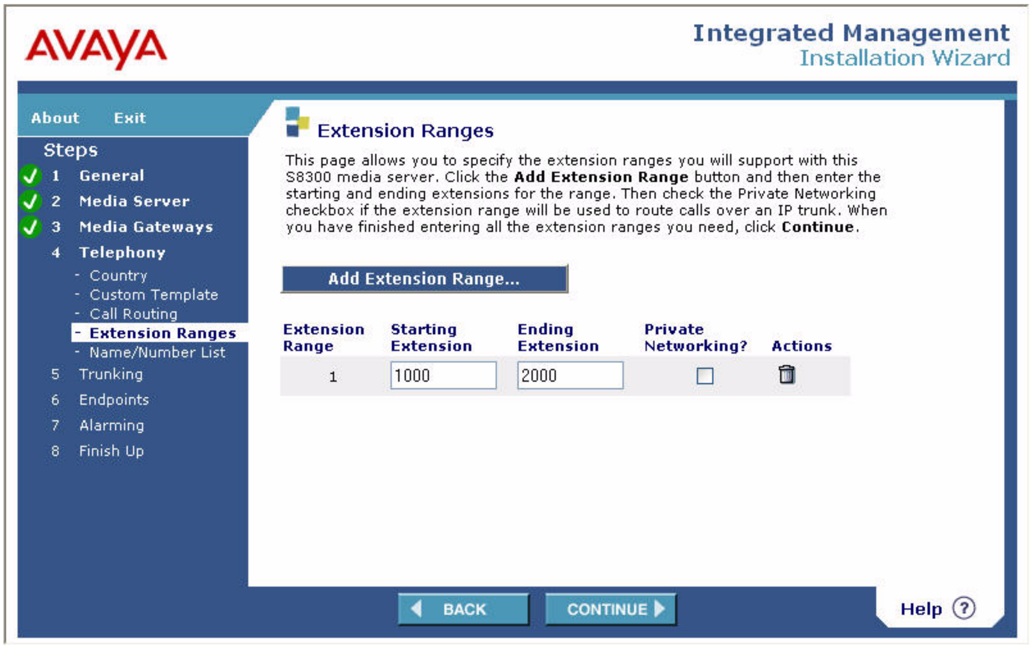
Other Local NPA(s) [ ] [ ] [ ] (Optional)

Attendant Access Number [ ] (0-9) (Optional)

Voice Mail Extension [ ] (Optional)

4. Click **Continue**.

   The **Extension Ranges** screen appears.



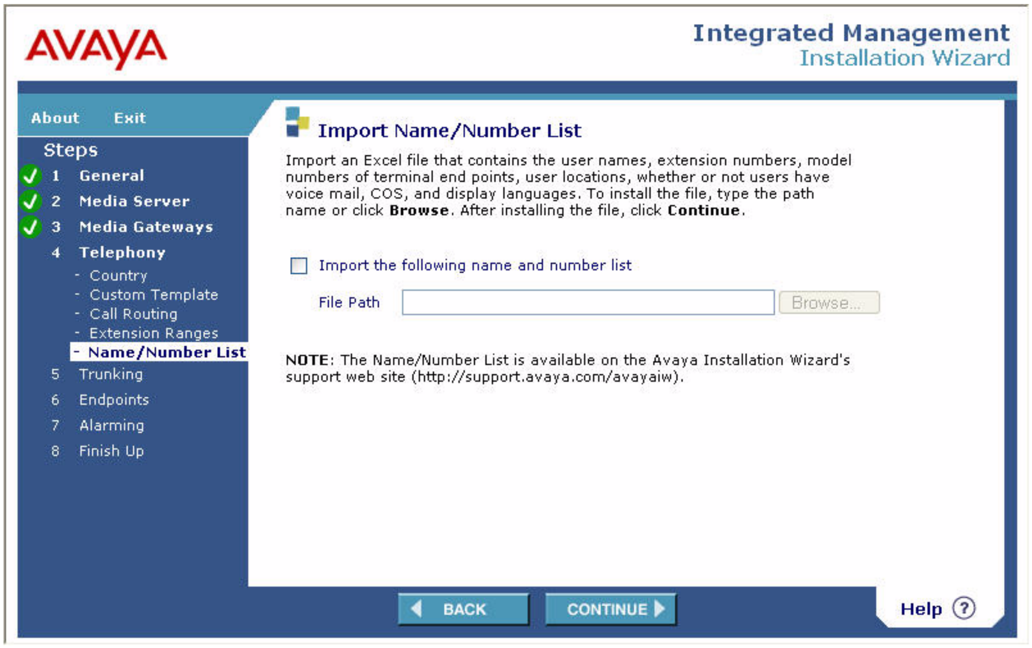
Extension Ranges

This page allows you to specify the extension ranges you will support with this S8300 media server. Click the **Add Extension Range** button and then enter the starting and ending extensions for the range. Then check the Private Networking checkbox if the extension range will be used to route calls over an IP trunk. When you have finished entering all the extension ranges you need, click **Continue**.

Extension Range	Starting Extension	Ending Extension	Private Networking?	Actions
1	1000	2000	□	🗑

5. To add a range, click **Add Extension Range** and enter the starting and ending extensions for the range. If you want this range to be used to route calls over an IP trunk, select **Private Networking**. To add additional extension ranges, repeat these steps. When you are finished, click **Continue**.

   The **Import Name/Number List** screen appears. This screen allows you to import an Excel file that contains user names, extension numbers, and other information.



Import Name/Number List

Import an Excel file that contains the user names, extension numbers, model numbers of terminal end points, user locations, whether or not users have voice mail, COS, and display languages. To install the file, type the path name or click **Browse**. After installing the file, click **Continue**.

☐ Import the following name and number list

File Path [ ] Browse...

NOTE: The Name/Number List is available on the Avaya Installation Wizard's support web site (http://support.avaya.com/avayaiw).

To import this file:

a. Select **Import the following name and number list**.

b. Enter the file path of the file you want to import, or use the **Browse** button to locate the file.

c. Click **Continue**.

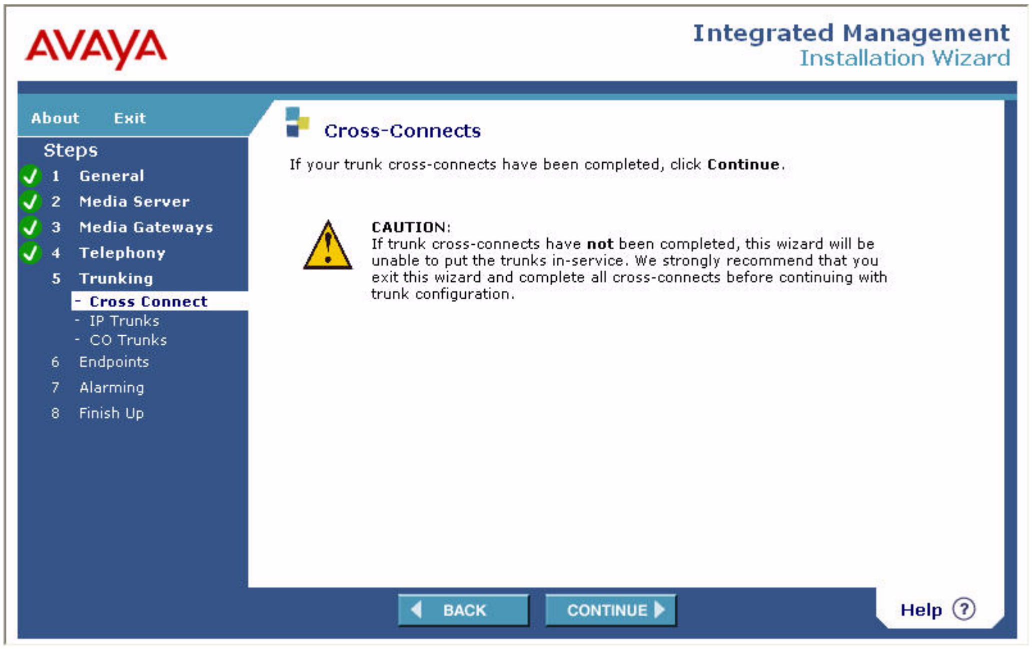
Trunk configuration

For trunk configuration:

1. To configure the trunk parameters of the media gateway, do one of the following:
   - From the **Import Name/Number List** screen, click **Continue**.

     or
   - Click **Trunking** from the main menu.

   The **Cross-Connects** screen appears. If you have completed the trunk cross-connects,click **Continue** to proceed with trunk configuration. If you have not completed the trunk cross-connects, Avaya recommends you to exit the Avaya Installation Wizard and complete all cross-connects before proceeding with trunk configuration.

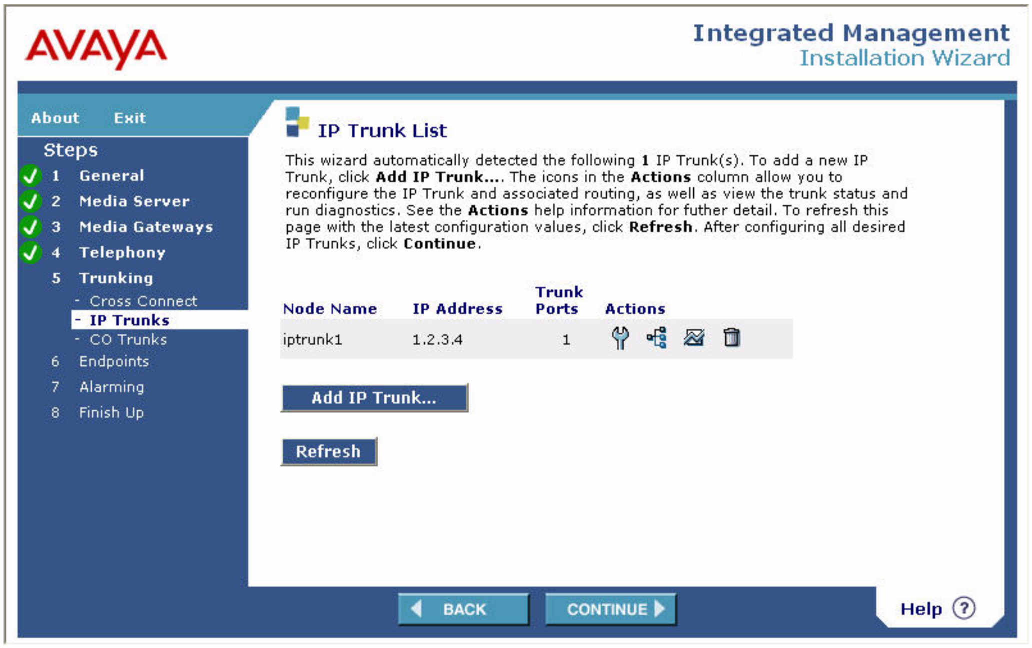


Cross-Connects

If your trunk cross-connects have been completed, click **Continue**.

CAUTION:
If trunk cross-connects have **not** been completed, this wizard will be unable to put the trunks in-service. We strongly recommend that you exit this wizard and complete all cross-connects before continuing with trunk configuration.

2. Click **Continue**. The **IP Trunk List** screen appears. This screen displays all IP trunks configured on the media gateway. To refresh this list, click **Refresh**.



IP Trunk List

This wizard automatically detected the following **1** IP Trunk(s). To add a new IP Trunk, click **Add IP Trunk...**. The icons in the **Actions** column allow you to reconfigure the IP Trunk and associated routing, as well as view the trunk status and run diagnostics. See the **Actions** help information for futher detail. To refresh this page with the latest configuration values, click **Refresh**. After configuring all desired IP Trunks, click **Continue**.

Node Name	IP Address	Trunk Ports	Actions
iptrunk1	1.2.3.4	1	

Add IP Trunk...

Refresh

3. You can perform the following actions in the **IP Trunk List** screen:

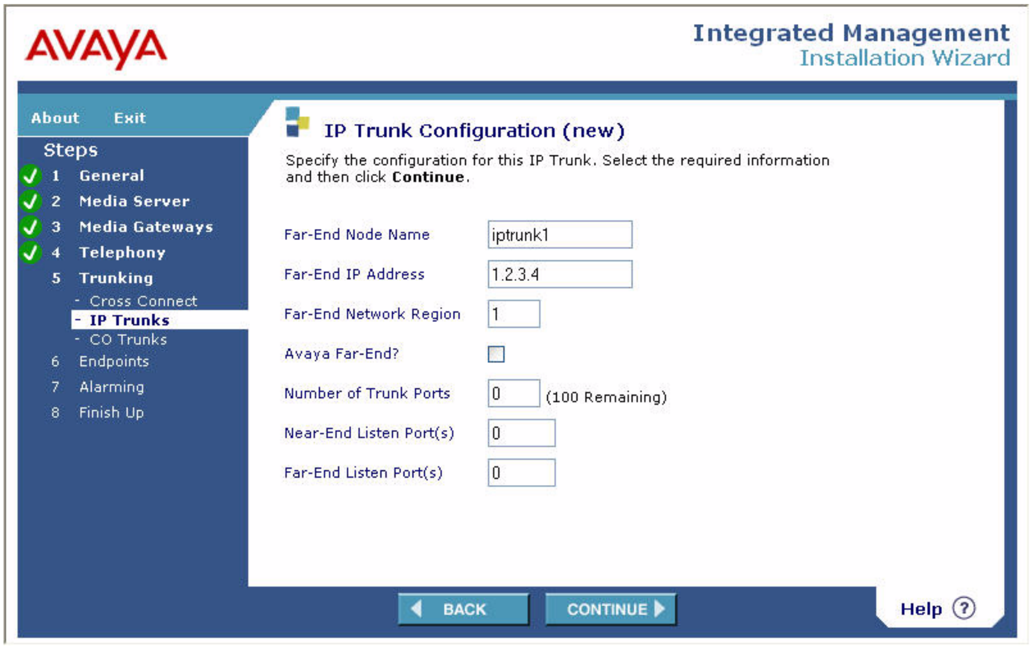
- Adding a trunk
- Modifying trunk parameters
- Modifying IP route configuration
- Displaying trunk status
- Removing a trunk

To proceed to the **CO Trunk List** screen for configuring a trunk media module, click **Continue**. See Configuring a trunk media module on page 154.

Adding a trunk

To add a new trunk:

1. Click **Add IP Trunk**. The **IP Trunk Configuration** screen appears.



IP Trunk Configuration (new)

Specify the configuration for this IP Trunk. Select the required information and then click **Continue**.

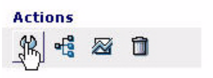
Far-End Node Name	iptrunk1
Far-End IP Address	1.2.3.4
Far-End Network Region	1
Avaya Far-End?	□
Number of Trunk Ports	0 (100 Remaining)
Near-End Listen Port(s)	0
Far-End Listen Port(s)	0

2. Enter the required information in the **IP Trunk Configuration** screen and click **Continue**. The IP Trunk List appears, with the new trunk included in the list of trunks. To add an additional trunk, click **Add IP Trunk** and repeat this step. When you are finished adding trunks, click **Continue** or select an action from the **Actions** column to modify an existing trunk.

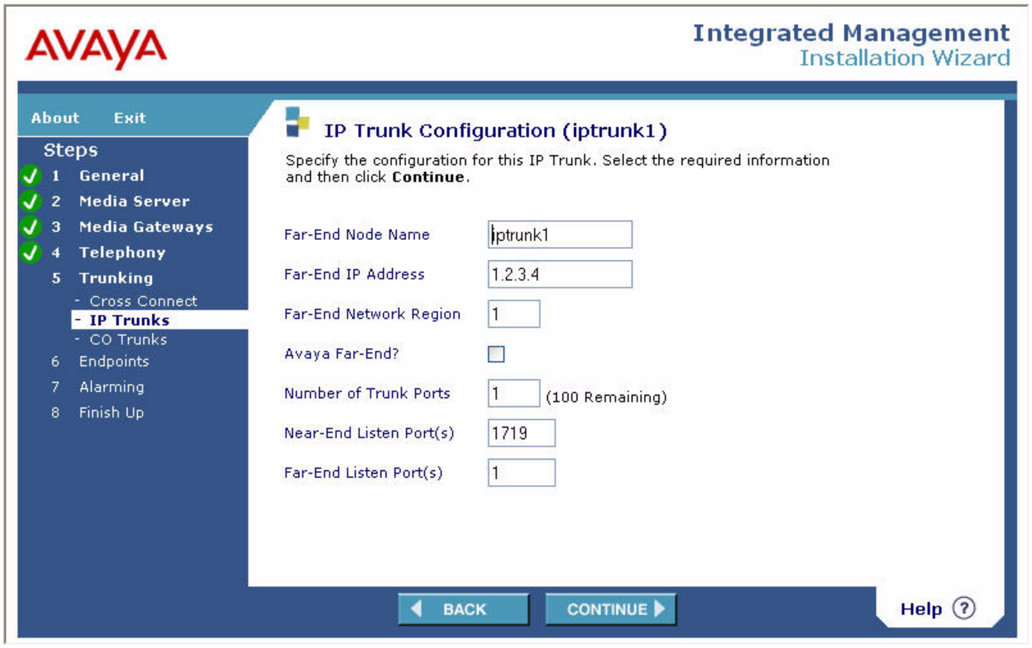
Modifying trunk parameters

To modify the trunk's parameters:

1. Click the configuration icon in the **Actions** column of the **IP Trunk List** screen.



The **IP Trunk Configuration** screen appears, with the trunk's current parameters displayed.



IP Trunk Configuration (iptrunk1)

Specify the configuration for this IP Trunk. Select the required information and then click **Continue**.

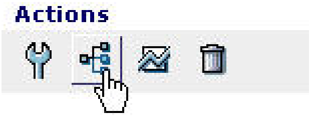
Far-End Node Name	iptrunk1
Far-End IP Address	1.2.3.4
Far-End Network Region	1
Avaya Far-End?	□
Number of Trunk Ports	1 (100 Remaining)
Near-End Listen Port(s)	1719
Far-End Listen Port(s)	1

2. Modify the trunk parameters and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the **CO Trunk List** screen. See Configuring a trunk media module on page 154.

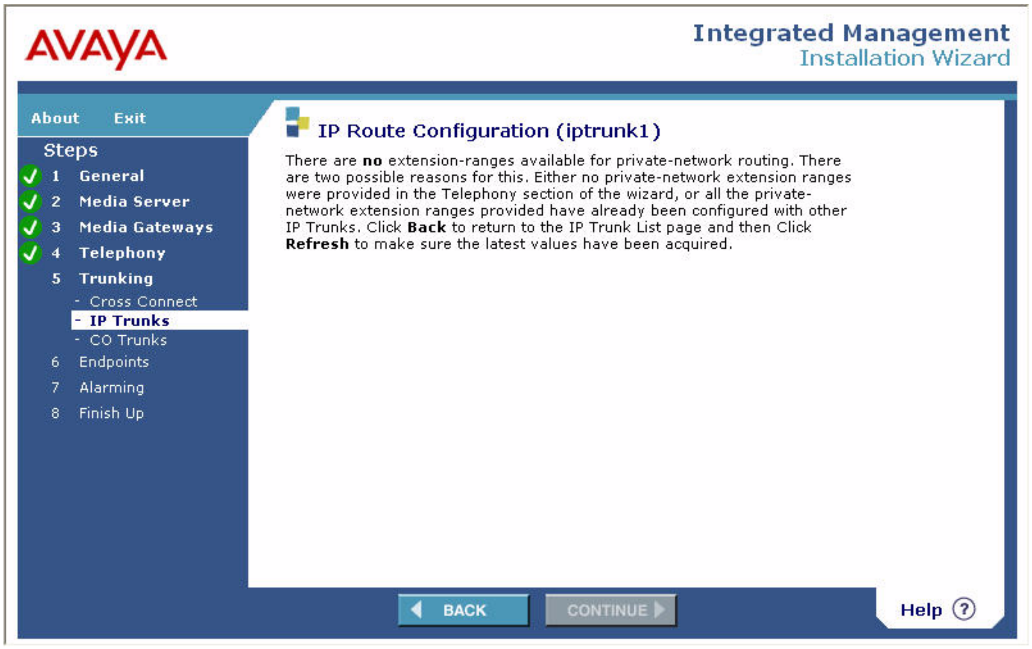
Modifying IP route configuration

To modify the trunk's IP route configuration:

1. Click the IP route icon in the **Actions** column of the **IP Trunk List** screen.



The **IP Route Configuration** screen appears.



IP Route Configuration (iptrunk1)

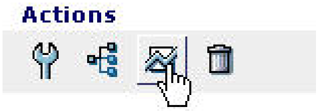
There are **no** extension-ranges available for private-network routing. There are two possible reasons for this. Either no private-network extension ranges were provided in the Telephony section of the wizard, or all the private-network extension ranges provided have already been configured with other IP Trunks. Click **Back** to return to the IP Trunk List page and then Click **Refresh** to make sure the latest values have been acquired.

2. The **IP Route Configuration** screen displays the extension ranges available for private-network routing. Modify these ranges, if any, and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the **CO Trunk List** screen. See Configuring a trunk media module on page 154.

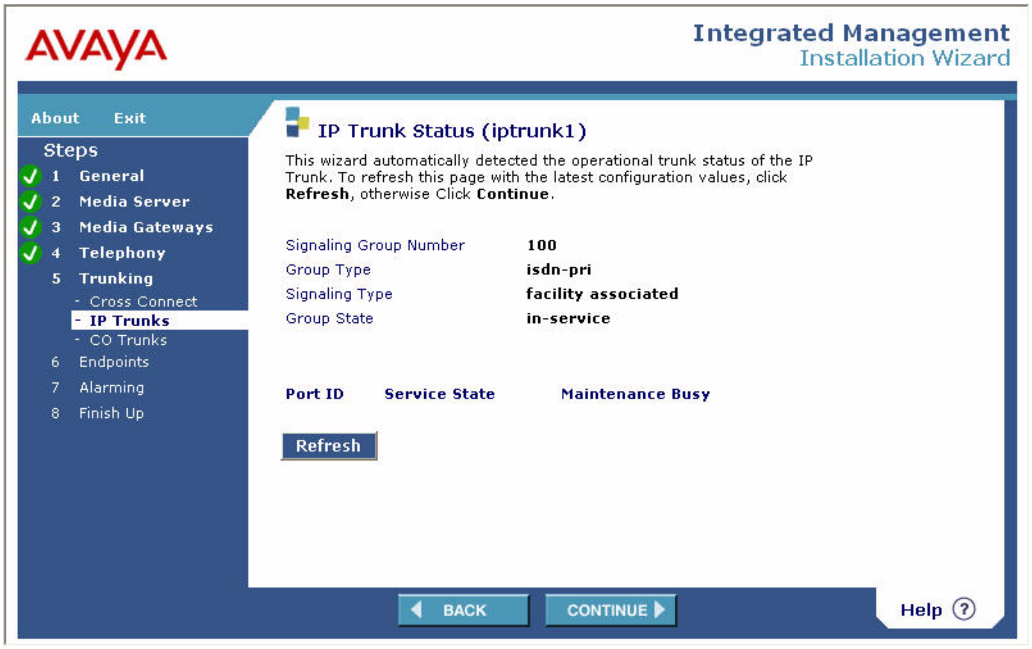
Displaying trunk status

To display the trunk's IP route configuration:

1. Click the trunk status icon in the **Actions** column of the **IP Trunk List** screen.



The **IP Trunk Status** screen appears.



IP Trunk Status (iptrunk1)

This wizard automatically detected the operational trunk status of the IP Trunk. To refresh this page with the latest configuration values, click **Refresh**, otherwise Click **Continue**.

Signaling Group Number	100
Group Type	isdn-pri
Signaling Type	facility associated
Group State	in-service

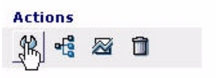
Port ID	Service State	Maintenance Busy

2. The **IP Trunk Status** screen displays the operational status of the trunk. To refresh the information, click **Refresh**. Otherwise, click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the **CO Trunk List** screen. See Configuring a trunk media module on page 154.

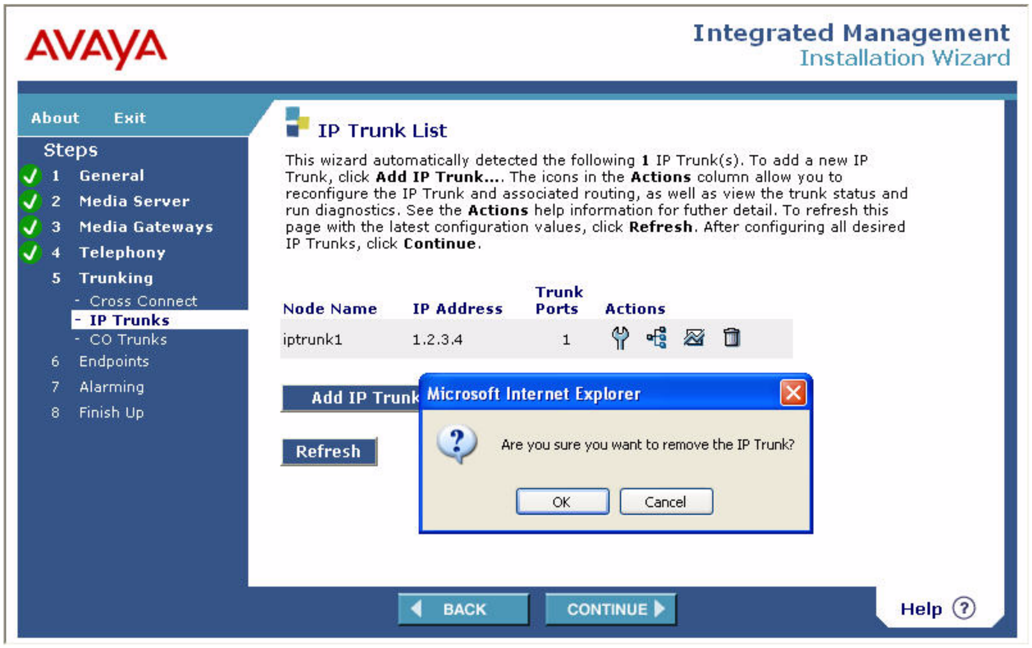
Removing a trunk

To remove a trunk:

1. Click the trunk's remove icon in the **Actions** column of the **IP Trunk List** screen.



A message appears asking if you want to remove the trunk.



IP Trunk List

This wizard automatically detected the following **1** IP Trunk(s). To add a new IP Trunk, click **Add IP Trunk...**. The icons in the **Actions** column allow you to reconfigure the IP Trunk and associated routing, as well as view the trunk status and run diagnostics. See the **Actions** help information for futher detail. To refresh this page with the latest configuration values, click **Refresh**. After configuring all desired IP Trunks, click **Continue**.

Node Name	IP Address	Trunk Ports	Actions
iptrunk1	1.2.3.4	1	

Microsoft Internet Explorer

Are you sure you want to remove the IP Trunk?

OK Cancel

2. Click **OK** to remove the trunk. Select an additional action from the **Actions** column, or click **Continue** to proceed to the **CO Trunk List** screen.

Configuring a trunk media module

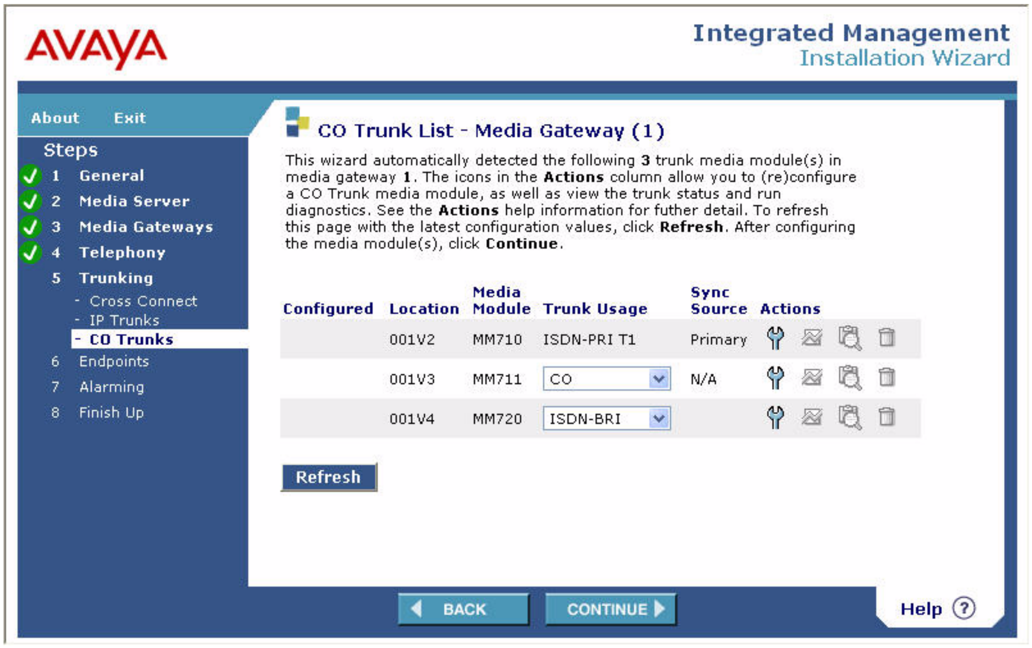
To configure a trunk media module, do one of the following:

- Click **Continue** from the **IP Trunk List** screen.

  or

- Select **Trunking > CO Trunks** from the main menu.

The **CO Trunk List** screen appears. This screen lists trunk media modules detected in the G700 and allows you to configure a media module and run diagnostics. To configure or run diagnostics on a trunk media module, click the Actions icon for the module.



CO Trunk List - Media Gateway (1)

This wizard automatically detected the following **3** trunk media module(s) in media gateway **1**. The icons in the **Actions** column allow you to (re)configure a CO Trunk media module, as well as view the trunk status and run diagnostics. See the **Actions** help information for futher detail. To refresh this page with the latest configuration values, click **Refresh**. After configuring the media module(s), click **Continue**.

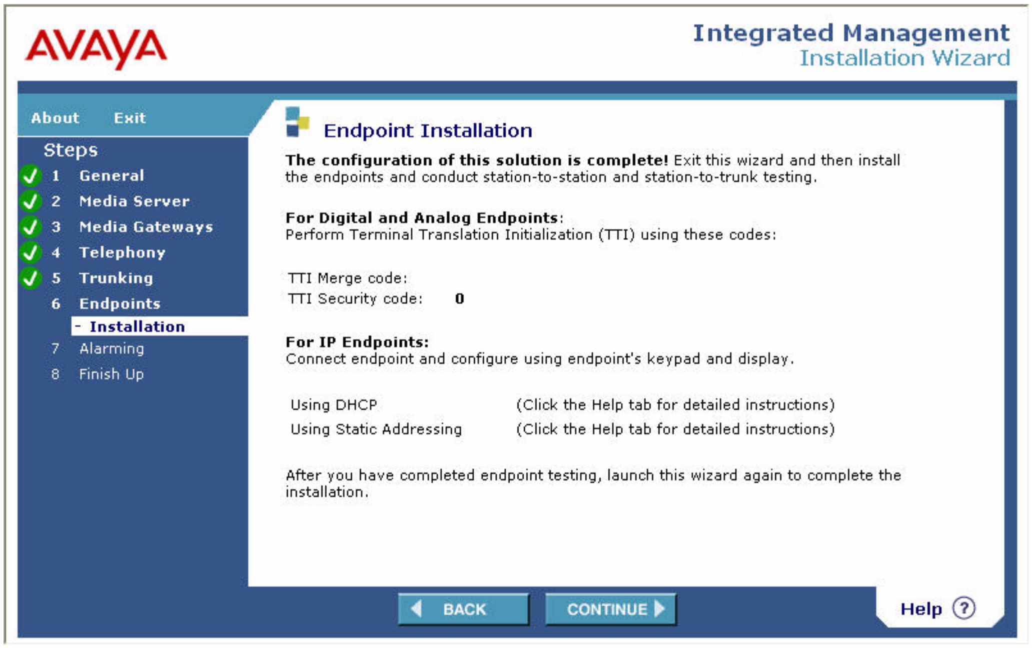
Configured	Location	Media Module	Trunk Usage	Sync Source	Actions
	001V2	MM710	ISDN-PRI T1	Primary	
	001V3	MM711	CO	N/A	
	001V4	MM720	ISDN-BRI		

Endpoint installation

For instructions on endpoint installation, do one of the following:

- Click **Continue** from the **CO Trunk List** screen, or
- Click **Endpoints** from the main menu.

The **Endpoint Installation** screen appears. You can access endpoint installation information from this screen.



Endpoint Installation

The configuration of this solution is complete! Exit this wizard and then install the endpoints and conduct station-to-station and station-to-trunk testing.

For Digital and Analog Endpoints:
Perform Terminal Translation Initialization (TTI) using these codes:

TTI Merge code:
TTI Security code: **0**

For IP Endpoints:
Connect endpoint and configure using endpoint's keypad and display.

Using DHCP	(Click the Help tab for detailed instructions)
Using Static Addressing	(Click the Help tab for detailed instructions)

After you have completed endpoint testing, launch this wizard again to complete the installation.

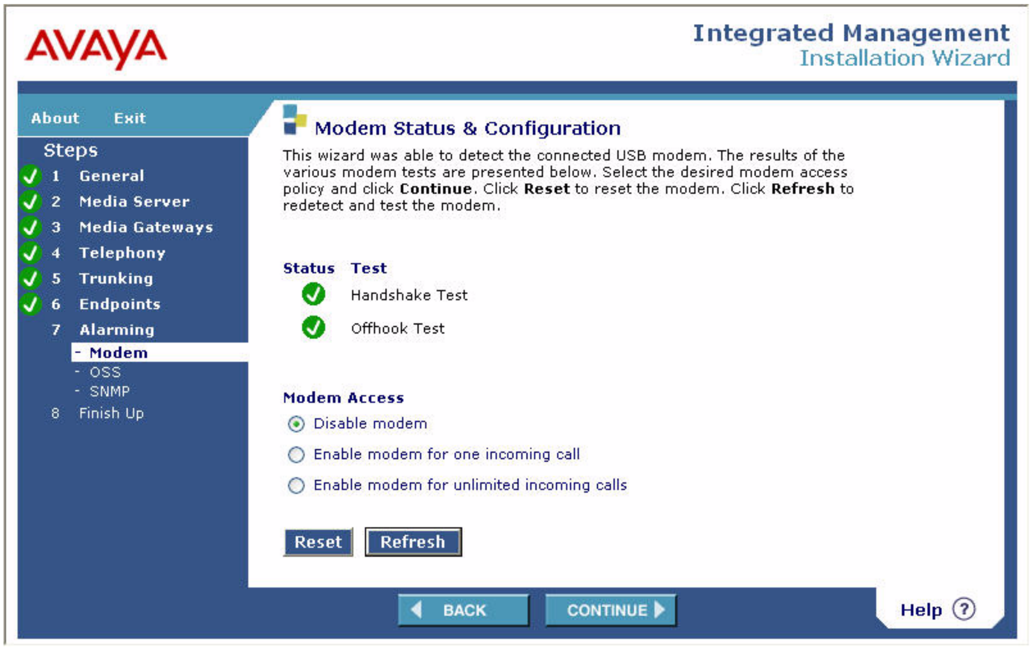
Alarm configuration

To display modem status and configure alarms:

1. Click **Alarming** from the main menu.

   The **Modem Status & Configuration** screen appears. This screen detects any modem connected to the media gateway. The screen also displays the results of tests performed on the modem. You can perform the following actions from this screen:

   - Click **Reset** to reset the modem.
   - Click **Refresh** to re-detect and test the modem.



Modem Status & Configuration

This wizard was able to detect the connected USB modem. The results of the various modem tests are presented below. Select the desired modem access policy and click **Continue**. Click **Reset** to reset the modem. Click **Refresh** to redetect and test the modem.

Status	Test
✓	Handshake Test
✓	Offhook Test

Modem Access

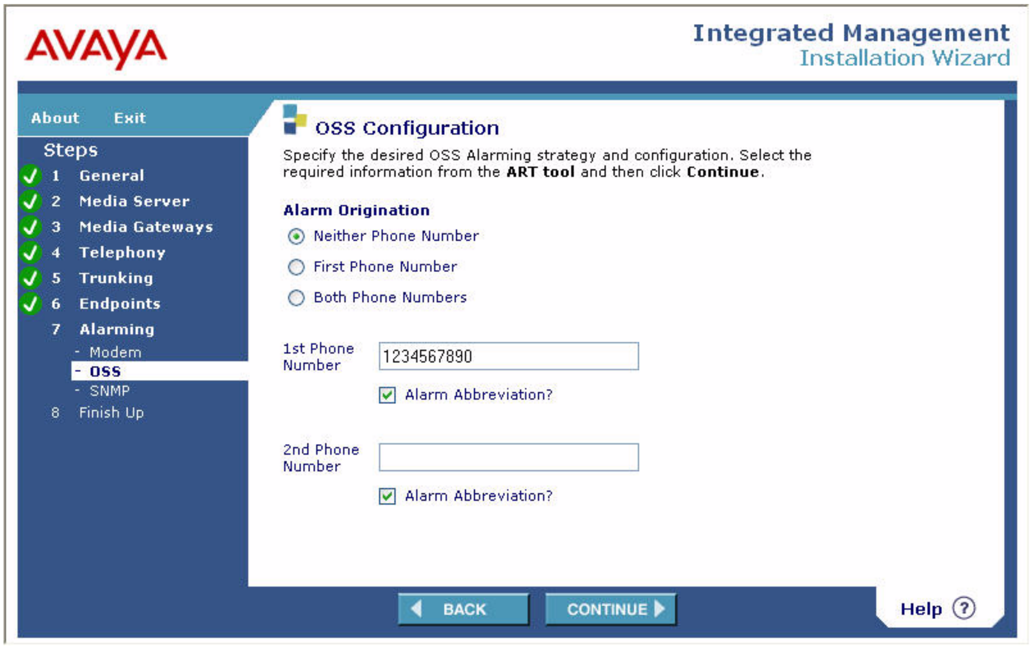
● Disable modem

○ Enable modem for one incoming call

○ Enable modem for unlimited incoming calls

2. Select the appropriate modem access policy in the **Modem Access** area and click **Continue**.

   The **OSS Configuration** screen appears.



OSS Configuration

Specify the desired OSS Alarming strategy and configuration. Select the required information from the **ART tool** and then click **Continue**.

Alarm Origination

● Neither Phone Number

○ First Phone Number

○ Both Phone Numbers

1st Phone Number: 1234567890

☑ Alarm Abbreviation?

2nd Phone Number:

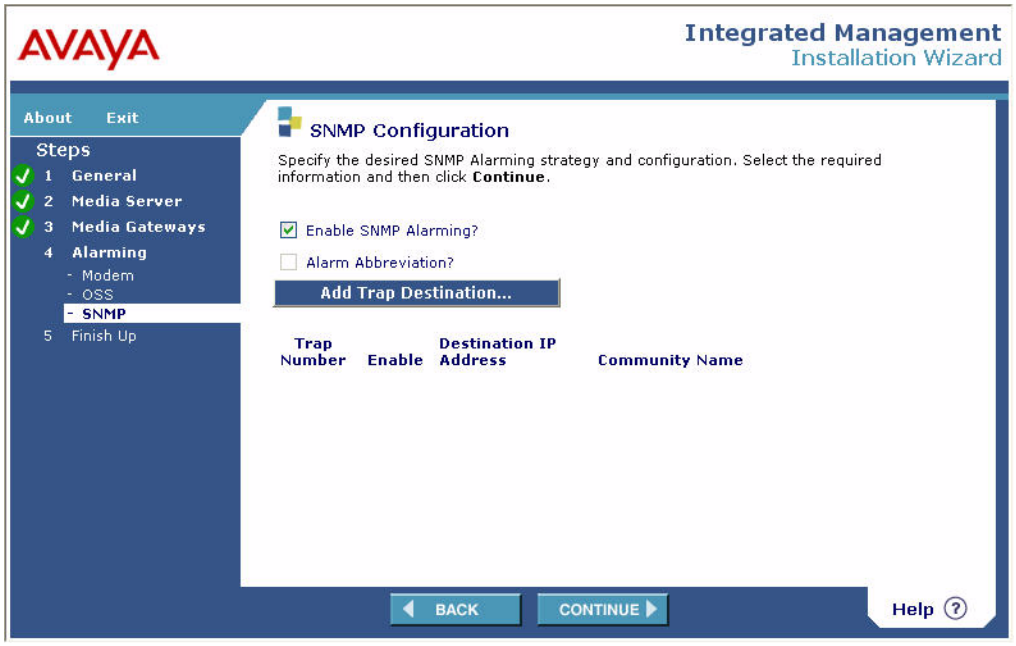
☑ Alarm Abbreviation?

3. Enter the required information from the ART tool. For information on using the ART tool, see Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary on page 118.

4. Click **Continue**.

   The **SNMP Configuration** screen appears.

5. Check Enable SNMP alarming if you want to enable the sending of SNMP traps to the INADS. In the Destination IP Address field, enter the INADS IP address. In the Community Name field, enter an SNMP community access string. Check the Alarm abbreviation checkbox if you want to enable SNMP alarm abbreviation.



SNMP Configuration

Specify the desired SNMP Alarming strategy and configuration. Select the required information and then click **Continue**.

☑ Enable SNMP Alarming?

□ Alarm Abbreviation?

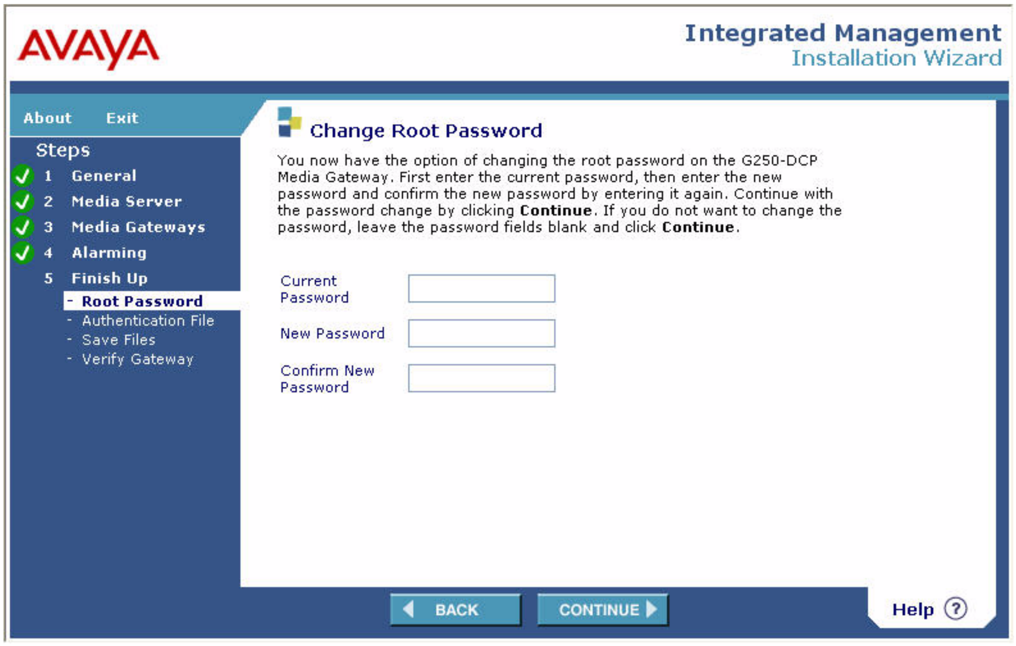
Trap Number	Enable	Destination IP Address	Community Name

Password and final screens

To change your password (optional) and complete the installation:

1. Click **Continue** from the **SNMP Configuration** screen.

   The **Change Root Password** screen appears. This screen allows you to change the root password on the media gateway.



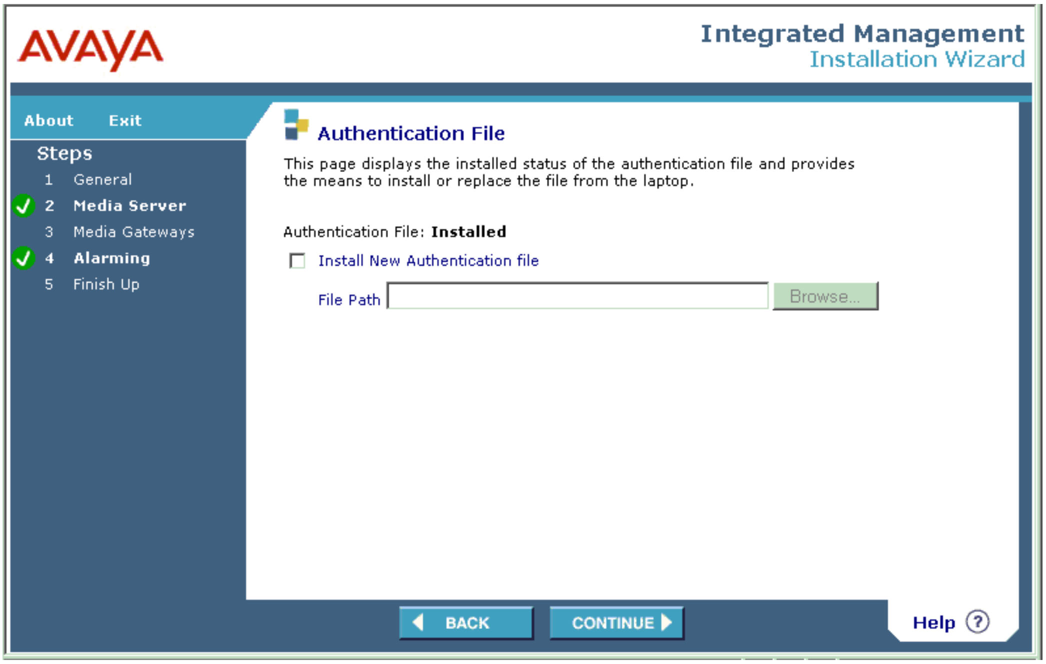
Change Root Password

You now have the option of changing the root password on the G250-DCP Media Gateway. First enter the current password, then enter the new password and confirm the new password by entering it again. Continue with the password change by clicking **Continue**. If you do not want to change the password, leave the password fields blank and click **Continue**.

Current Password	
New Password	
Confirm New Password	

2. Click **Continue**.

   The **Authentication File** screen appears if there is a resident server on the gateway and if you selected **Translations will be added after the installation has been completed using the SAT, ProVision, ASA or another Integrated Management tool** in the **Translation Source** screen. The **Authentication File** screen allows you to install the authentication file for access to the S8300 Server.



Authentication File

This page displays the installed status of the authentication file and provides the means to install or replace the file from the laptop.

Authentication File: **Installed**

□ Install New Authentication file

File Path [ ] Browse...

3. Click **Install New Authentication File**.
4. Click the **Browse** button to locate the authentication file on your laptop.
5. Click **Continue.**

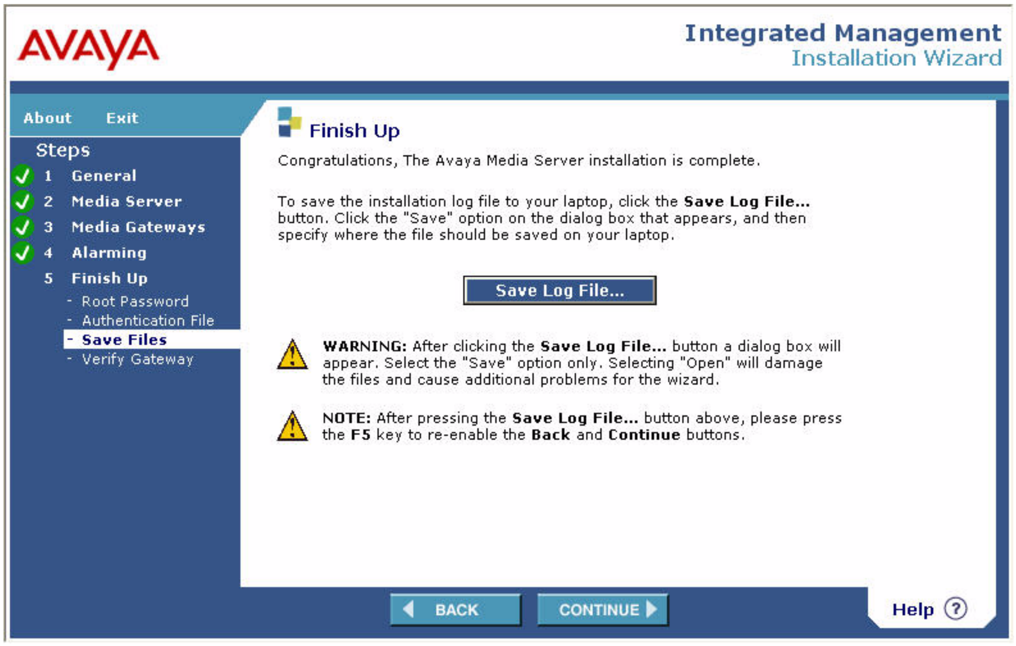
   The **Finish Up** screen appears. This screen allows you to save the installation log file to your laptop. To save the installation log file:

   a. Click **Save Log File**. A dialog box appears.

   b. Click **Save**.

   WARNING:
   Do not click **Open**. Clicking **Open** will damage the log file and may cause other problems to the Avaya IW.

   c. Press **<F5>** to restore the **Back** and **Continue** buttons to the **Finish Up** screen.



Finish Up

Congratulations, The Avaya Media Server installation is complete.

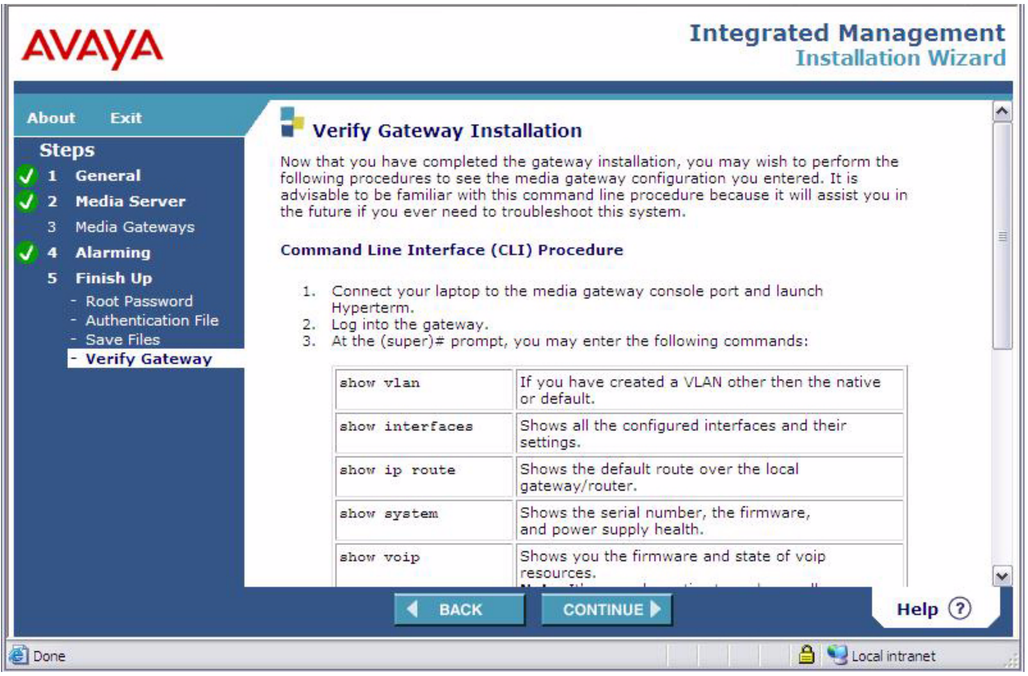
To save the installation log file to your laptop, click the **Save Log File...** button. Click the "Save" option on the dialog box that appears, and then specify where the file should be saved on your laptop.

WARNING: After clicking the **Save Log File...** button a dialog box will appear. Select the "Save" option only. Selecting "Open" will damage the files and cause additional problems for the wizard.

NOTE: After pressing the **Save Log File...** button above, please press the **F5** key to re-enable the **Back** and **Continue** buttons.

6. Click **Continue**.

   The **Verify Gateway Installation** screen appears. This screen displays a list of CLI commands that you can use to verify the G700 configuration. The following figure shows a portion of the **Verify Gateway Installation** screen.



Verify Gateway Installation

Now that you have completed the gateway installation, you may wish to perform the following procedures to see the media gateway configuration you entered. It is advisable to be familiar with this command line procedure because it will assist you in the future if you ever need to troubleshoot this system.

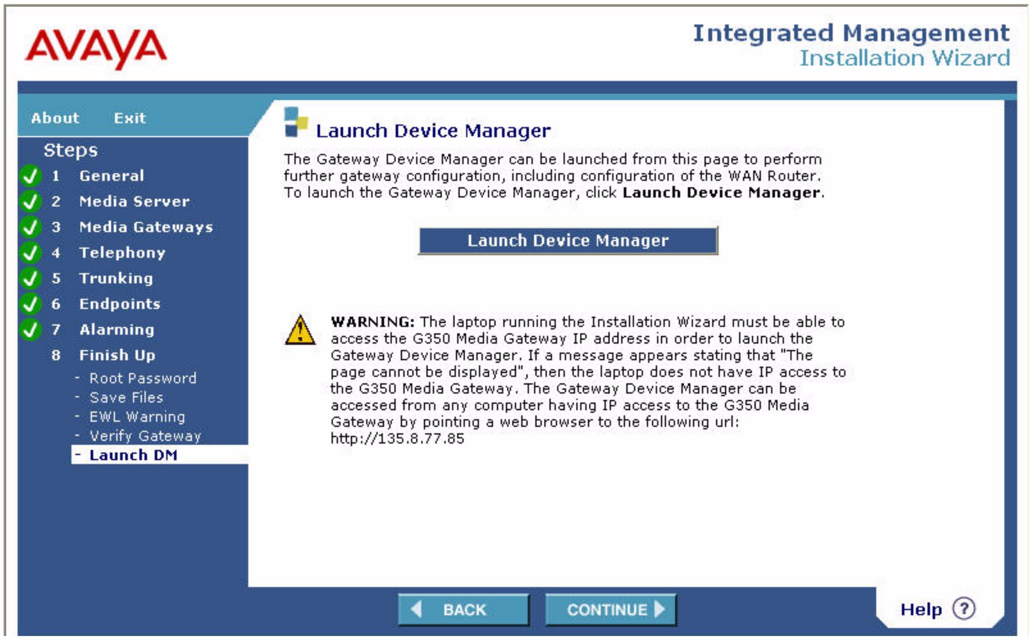
Command Line Interface (CLI) Procedure

1. Connect your laptop to the media gateway console port and launch Hyperterm.
2. Log into the gateway.
3. At the (super)# prompt, you may enter the following commands:

`show vlan`	If you have created a VLAN other then the native or default.
`show interfaces`	Shows all the configured interfaces and their settings.
`show ip route`	Shows the default route over the local gateway/router.
`show system`	Shows the serial number, the firmware, and power supply health.
`show voip`	Shows you the firmware and state of voip resources.

7. Click **Continue**.

   The **Launch Device Manager** screen appears. This screen allows you to launch the Gateway Device Manager.

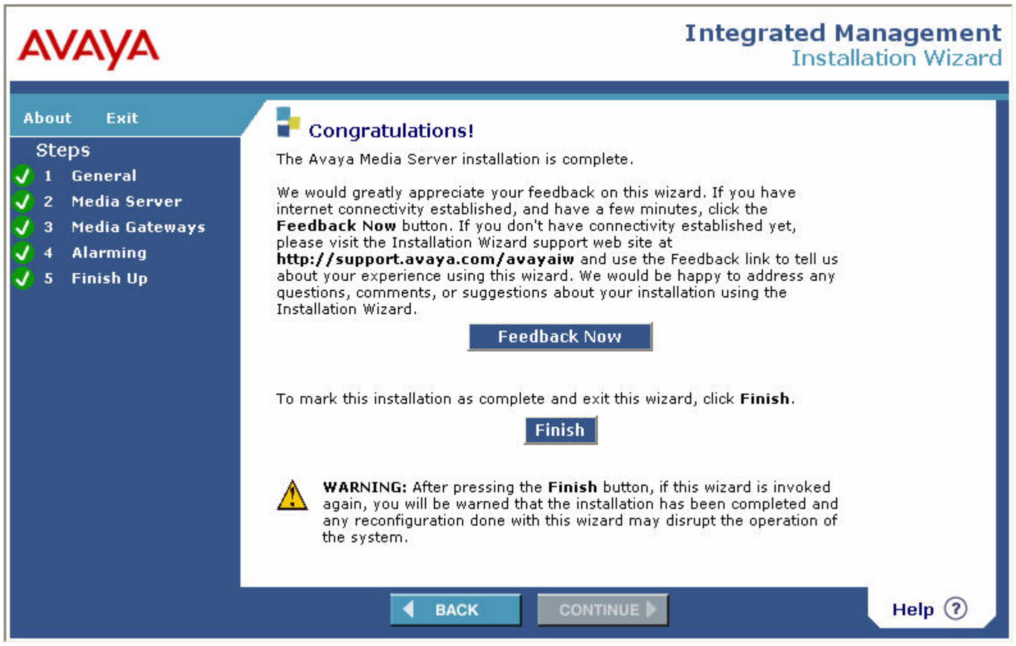


Launch Device Manager

The Gateway Device Manager can be launched from this page to perform further gateway configuration, including configuration of the WAN Router. To launch the Gateway Device Manager, click **Launch Device Manager**.

WARNING: The laptop running the Installation Wizard must be able to access the G350 Media Gateway IP address in order to launch the Gateway Device Manager. If a message appears stating that "The page cannot be displayed", then the laptop does not have IP access to the G350 Media Gateway. The Gateway Device Manager can be accessed from any computer having IP access to the G350 Media Gateway by pointing a web browser to the following url: http://135.8.77.85

8. Click **Continue**. The **Congratulations**! screen appears to inform you that the installation is complete. To exit the Avaya Installation Wizard, click **Finish**.



Congratulations!

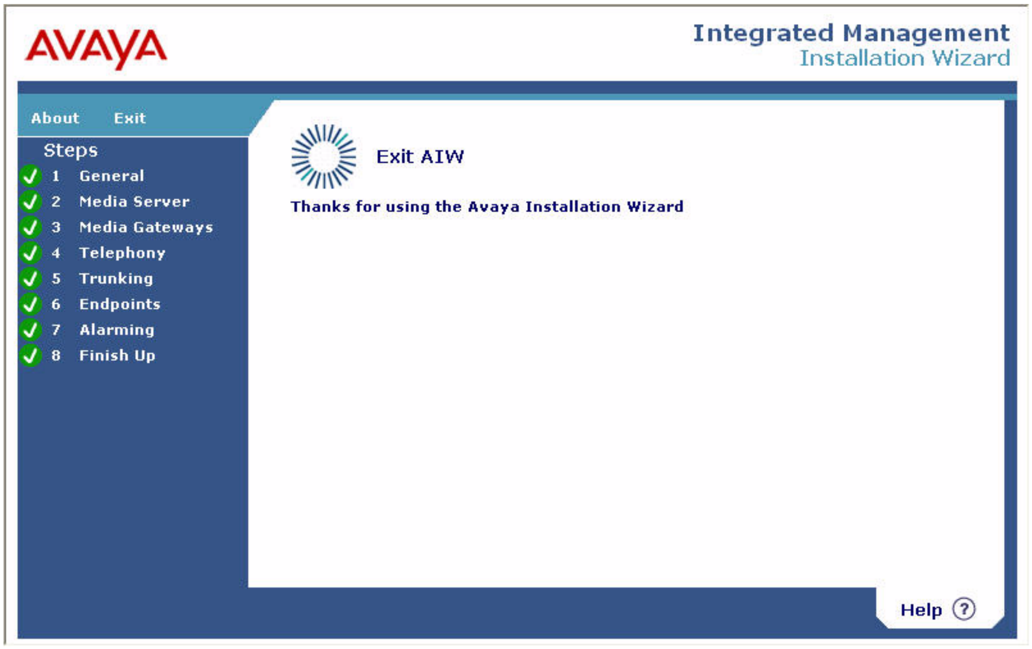
The Avaya Media Server installation is complete.

We would greatly appreciate your feedback on this wizard. If you have internet connectivity established, and have a few minutes, click the **Feedback Now** button. If you don't have connectivity established yet, please visit the Installation Wizard support web site at **http://support.avaya.com/avayaiw** and use the Feedback link to tell us about your experience using this wizard. We would be happy to address any questions, comments, or suggestions about your installation using the Installation Wizard.

To mark this installation as complete and exit this wizard, click **Finish**.

WARNING: After pressing the **Finish** button, if this wizard is invoked again, you will be warned that the installation has been completed and any reconfiguration done with this wizard may disrupt the operation of the system.

9. The **Exit AIW** screen appears.



Exit AIW

Thanks for using the Avaya Installation Wizard

If you set date or time, reboot the server

The date and the time is set in the Avaya Installation Wizard. If you set the time, date, or time zone, you must reboot the server after Avaya Installation Wizard completes.

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

You will be logged off the server when it reboots. You can use ping to verify when the server is accessible again.

If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server’s command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`.
3. Type `start -ca`.

Enabling SIP Enablement Services, if required

If the S8300, as a primary controller only, is going to use SIP Enablement Services (SES), perform this task.

To enable SES

1. On the **Server (Maintenance)** Web page, select **Miscellaneous > SES Software**.

   The **SES Software** screen appears, and the text "SES is disabled" appears just above the **Enable SES** button.

2. Click **Enable SES**.

3. Wait approximately 30 seconds and click the refresh button on your browser.

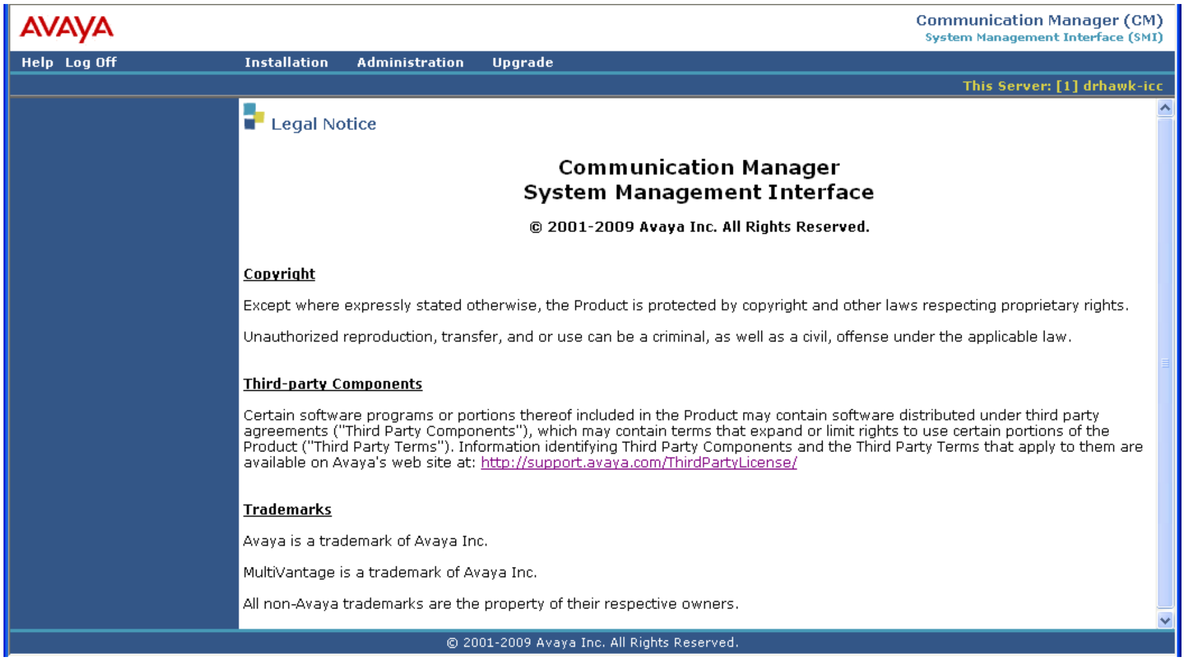
   The **SES Software** page should show "SES is enabled."

To verify SES is enabled

1. Return to the System Manager Interface Web page and refresh your browser.

2. On the **Administration** menu, verify that the **SIP Enablement Services** option is now available.

Communication Manager System Management Interface


AVAYA
Communication Manager (CM)
System Management Interface (SMI)
Help
Log Off
Installation
Administration
Upgrade
This Server: [1] drhawk-icc
Legal Notice

Communication Manager
System Management Interface

© 2001-2009 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

© 2001-2009 Avaya Inc. All Rights Reserved.

Note:

You must also install the SES license and administer SES. See Installing the SES license on page 187 and SES administration tasks on page 189.

Administering an S8300 primary controller

⚠ **CAUTION:**

This administration applies *only* to an S8300 primary controller, which may be the S8300 Server resident in a media gateway you are installing or may be an *external* S8300 Server somewhere else in the customer's network.

If the S8300 Server you just installed is configured as an LSP, do *not* perform this administration on it. Translations are automatically copied to this LSP from the external S8300 primary controller.

Skip this section and go to Administering an S8400, S8500, or S8700-series primary controller when the S8300 is an LSP on page 172 if the primary controller is an S8400, S8500, or S8700-series Server.

For the majority of administration required, see *Administering Avaya Aura™ Communication Manager*, 03-300509, or *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

In this section, you will use the SAT interface to:

- Assigning node names and IP addresses for the LSPs
- Administering Network Regions
- Administering IP Interfaces
- Identifying LSPs to the S8300 primary controller
- Associating LSPs with Network Regions

⚠ **CAUTION:**

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the system

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Log in, and open a SAT session (type **sat** or **dsat**).
3. At the SAT prompt, type **`reset system 4`**

   The system reboots.
4. After the reboot is complete, SSH to the S8300, login, and open a SAT session.

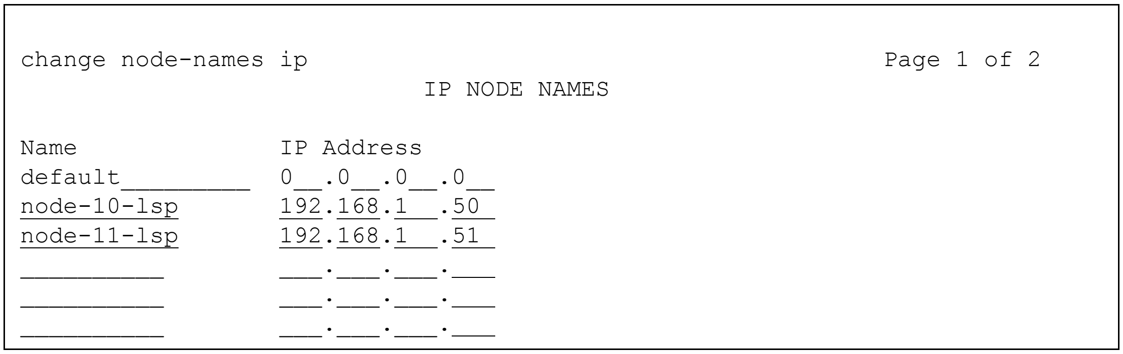
Assigning node names and IP addresses for the LSPs

If the S8300 network configuration includes LSPs, they must be specified on the **Node Names** screen.

To assign node names

1. At the S8300 SAT prompt, type **`change node-names ip`** to open the **Node Names** screen.

Example Node Names Screen



```
change node-names ip                                        Page 1 of 2
                             IP NODE NAMES

Name                 IP Address
default_________     0__.0__.0__.0__
node-10-lsp          192.168.1  .50
node-11-lsp          192.168.1  .51
__________           ___.___.___.___
__________           ___.___.___.___
__________           ___.___.___.___
```

2. Enter the name and IP addresses for the LSPs.
3. Press **F3** (**Enter**) when complete.

Administering Network Regions

Before assigning an IP network region to a media gateway, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

The number of network regions possible for an S8300 Server placed in a media gateway depends on the media gateway. For example, with a particular media gateway with an S8300 as primary controller, there will usually be one network region, defined as **1**.

The procedure below uses 1 for the network region number as an example but the procedure applies for any network region number from 1 to 250.

To define IP network region 1

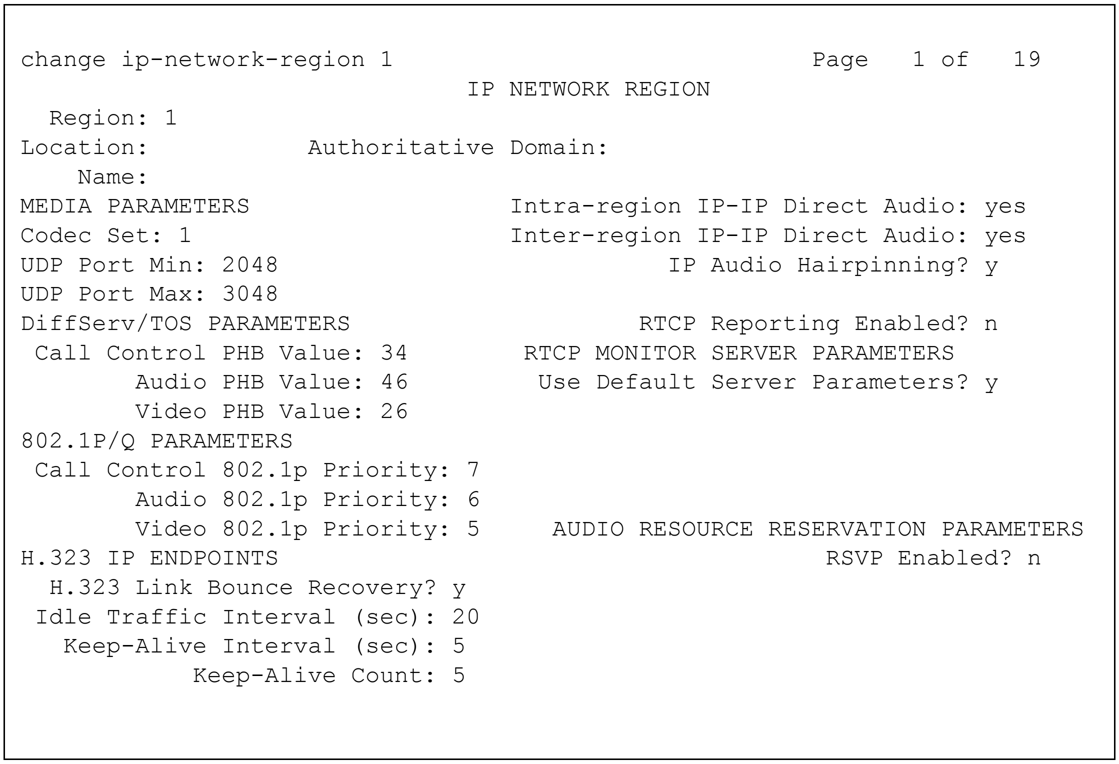
CAUTION:

Defining IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see "*Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504."

1. At the SAT prompt, type **`change ip-network-region 1`**.

   The S8300 displays the **IP Network Region** screen.

IP Network Region Screen



```
change ip-network-region 1                             Page   1 of   19
                               IP NETWORK REGION
  Region: 1
Location:           Authoritative Domain:
    Name:
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
Codec Set: 1                      Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                           IP Audio Hairpinning? y
UDP Port Max: 3048
DiffServ/TOS PARAMETERS                    RTCP Reporting Enabled? n
 Call Control PHB Value: 34        RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46         Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

2. If necessary, complete the fields as described in *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

   Note:

   It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

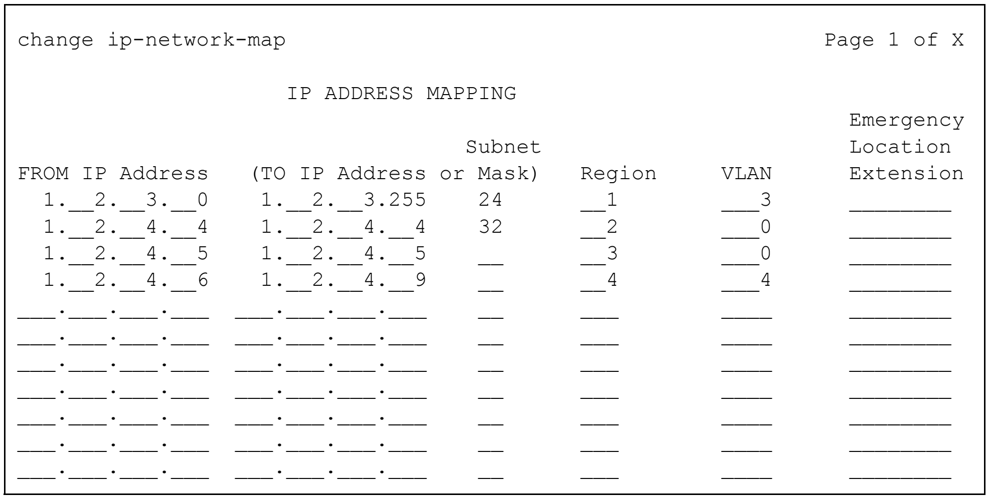
3. Press **F3** (**Enter**) to submit the screen.

Administering the IP address map

Administer the IP address map to assign IP phones and other IP endpoints to the same network region as the media gateway.

1. Type **`change ip-network-map`** and press **Enter** to display the **IP Address Mapping** screen.

IP Address Mapping Screen



```
change ip-network-map                                          Page 1 of X

                     IP ADDRESS MAPPING
                                                                 Emergency
                                 Subnet                          Location
FROM IP Address   (TO IP Address or Mask)   Region     VLAN      Extension
  1.__2.__3.__0    1.__2.__3.255    24       __1        ___3      ________
  1.__2.__4.__4    1.__2.__4.__4    32       __2        ___0      ________
  1.__2.__4.__5    1.__2.__4.__5    __       __3        ___0      ________
  1.__2.__4.__6    1.__2.__4.__9    __       __4        ___4      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
___.___.___.___  ___.___.___.___    __       ___        ____      ________
```

2. In the **FROM IP Address** and **TO IP Address** fields, enter a range of IP addresses for IP phones or other IP endpoints connected to the media gateway.
3. In the **Region** field, enter the network region to which the media gateway and its IP endpoints are to be assigned.
4. In the **VLAN** field, enter the VLAN number the IP endpoints should be a member of. Each network region should have its own VLAN number.
5. Enter an extension number in **Emergency Location Extension** field.

Note:

For more detail about the IP Address Mapping form, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Administering IP Interfaces

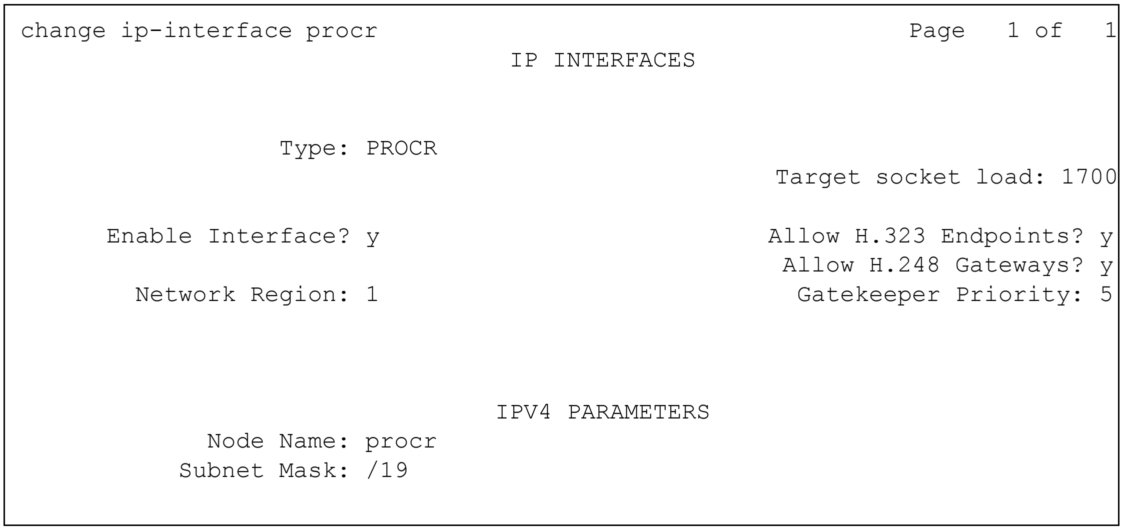
This procedure assigns network region 1, as an example, to the S8300 Server.

To assign the network region and IP endpoint access to the S8300

1. At the SAT prompt, type **`change ip-interfaces procr`**.

   The S8300 displays the **IP Interfaces** screen for the S8300 Server.

IP Interfaces Screen



```
change ip-interface procr                                    Page   1 of   1
                                  IP INTERFACES


                  Type: PROCR
                                                    Target socket load: 1700

      Enable Interface? y                          Allow H.323 Endpoints? y
                                                    Allow H.248 Gateways? y
        Network Region: 1                            Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /19
```

2. The field **Enable Ethernet?** should indicate `y` (yes)**.** The **Node Name** should be the IP address of the S8300 Server.
3. In the **Allow H.323 Endpoints** field, enter y to allow H.323 endpoint connectivity to the server.
4. In the **Allow H.248 Endpoints** field, enter y to allow H.248 media gateway connectivity to the server.
5. In the **Gatekeeper Priority** field, enter a value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to **y**.
6. In the **Target Socket Load** field, enter the maximum number of sockets targeted for this interface. The default is 80% of the maximum of 2000. When all the IP interfaces within the same Gatekeeper Priority exceeds the target number that you allocate, the system continues to add sockets until the interface is at its maximum capacity.

Identifying LSPs to the S8300 primary controller

If the primary controller has LSPs, you must enter the LSP node names on the Survivable Processor form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the survivable-processor screen, their status can be viewed with the **`list survivable-processor`** command.

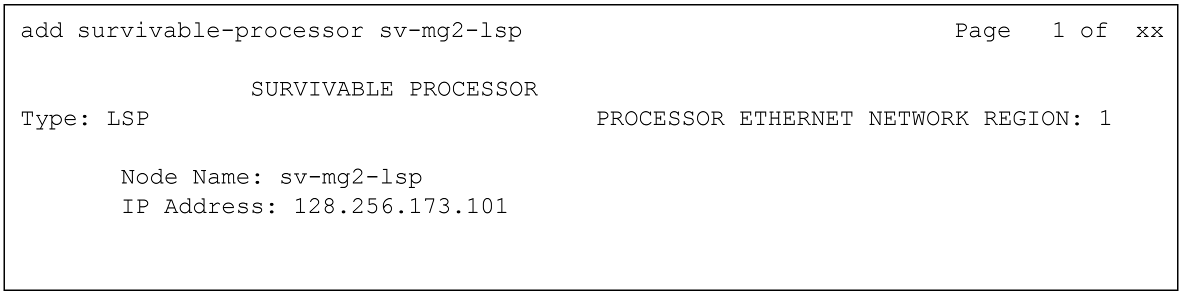
Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **Survivable Processor** screen.

1. At the SAT command line, type **`add survivable-processor`** ***<name>,*** where ***<name>*** is the LSP name from the **Node Names** screen.

   The **Survivable Processor** screen appears.

Figure 14: Add Local Survivable Processor screen



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

                SURVIVABLE PROCESSOR
Type: LSP                               PROCESSOR ETHERNET NETWORK REGION: 1

       Node Name: sv-mg2-lsp
       IP Address: 128.256.173.101
```

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Node Name is a display-only field that shows the name used to identify this server. You enter node names through the IP Node Names screen.
4. IP Address is a display-only field that shows the IP address that corresponds to the node name you entered.
5. Enter a Processor Ethernet Network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support. Valid values can be from 1 to250. Enter the network region in which the PE interface of the LSP resides.

Associating LSPs with Network Regions

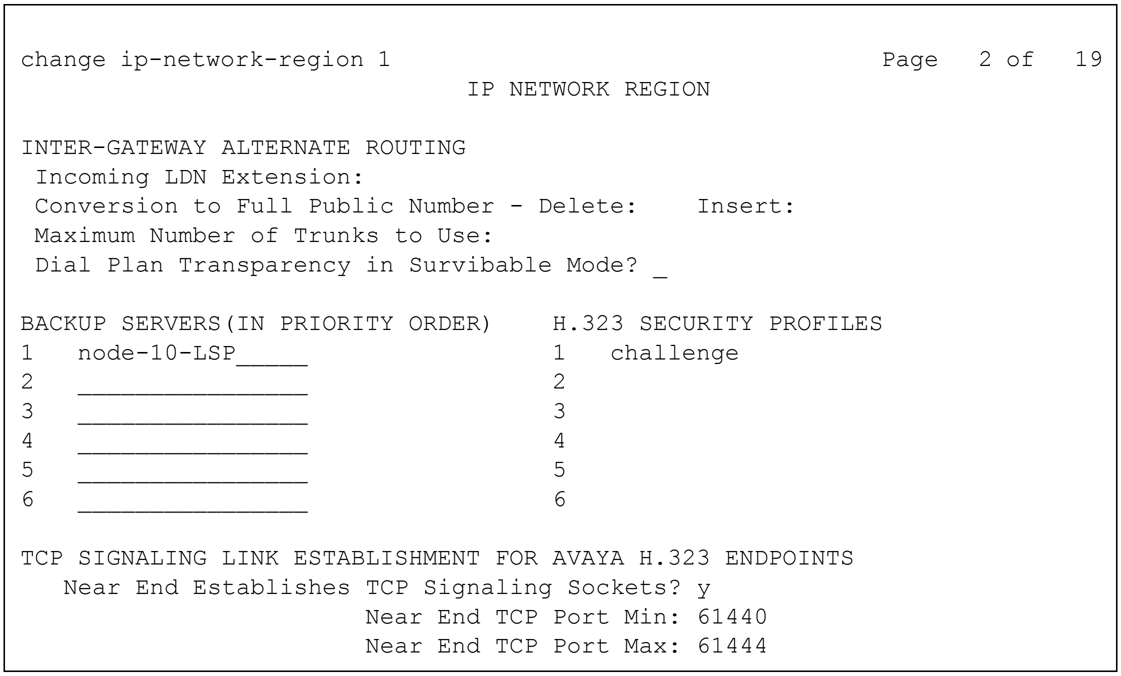
If the primary controller has LSPs, you can associate each LSP with one or more network regions. In the event of a network failure, IP telephones assigned to a network region will register with an LSP associated with that region.

This procedure associates up to six LSPs with a network region.

To associate LSPs with a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2



```
change ip-network-region 1                                  Page   2 of   19
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING
 Incoming LDN Extension:
 Conversion to Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use:
 Dial Plan Transparency in Survivable Mode? _

BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES
1   node-10-LSP_____                 1   challenge
2   ________________                 2
3   ________________                 3
4   ________________                 4
5   ________________                 5
6   ________________                 6

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Sockets? y
                        Near End TCP Port Min: 61440
                        Near End TCP Port Max: 61444
```

2. Enter the names of up to six LSPs to be associated with region 1.

   The LSP names must be the same as administered on the **Node Names** screen.

3. Submit the form.

4. Repeat for each network region with which you want to associate LSPs.

Skip to Administering the Media Gateway with S8300 Server on page 182.

Administering an S8400, S8500, or S8700-series primary controller when the S8300 is an LSP

In this case, the S8300 you have installed is configured as an LSP.

⚠ **CAUTION:**

This administration applies only to the primary controller that controls the S8300 LSP that you are installing. The primary controller can be an S8400, S8500, or S8700-series Server. Do *not* administer the S8300 LSP. Translations are automatically copied to the LSP from the primary controller.

Skip this section and go to Administering an S8300 primary controller on page 165 if the primary controller is an S8300.

Note:

Some of the procedures in this section may have been completed previously as part of a normal server installation.

For the majority of required administration, see *Administering Avaya Aura™ Communication Manager*, 03-300509, or *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

In this section, you will use the SAT interface on the primary controller to:

- Assigning Node Names and IP Addresses for the C-LANs and LSPs
- Administering Network Regions
- Administering IP Interfaces
- Identifying the Survivable Processor on the primary controller
- Assigning LSPs with Network Regions

Note:

For information on installing the C-LAN boards on the S8400, S8500, or S8700-series port networks and complete information on installing an S8400, S8500, or S8700-series Server, see the Installation documentation on the *Documentation for Avaya Aura™ Communication Manager, Media Gateways and Servers CD*, 03-300151.

Assigning Node Names and IP Addresses for the C-LANs and LSPs

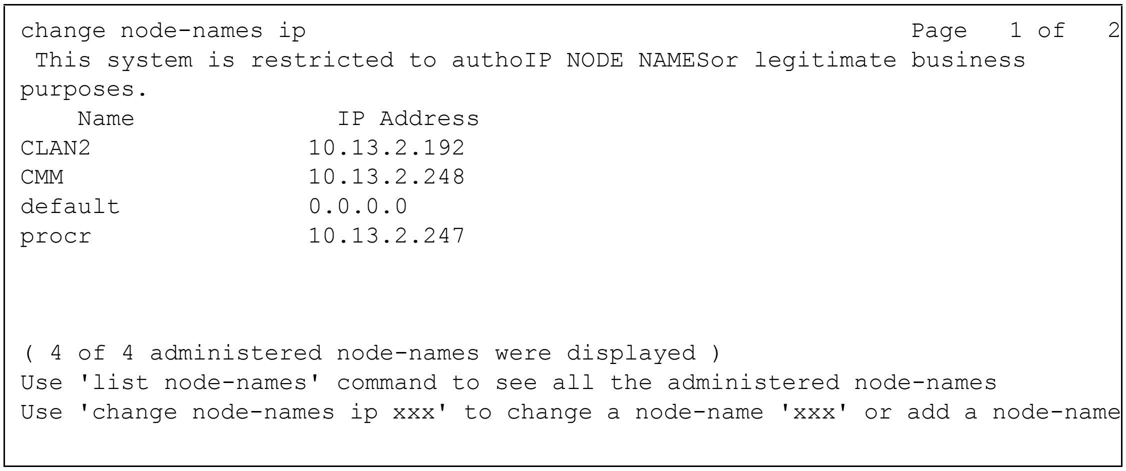
Note:

The C-LAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the server. For information on how to upgrade the firmware on the S8400, S8500 or S8700-series Server, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Servers and Gateways*, 03-300412.

To assign node names and IP addresses

1. At the SAT prompt, type **`change node-names ip`** to open the **Node Names** screen.

Example Node Names Screen



```
change node-names ip                                          Page   1 of   2
 This system is restricted to authoIP NODE NAMESor legitimate business
purposes.
    Name              IP Address
CLAN2               10.13.2.192
CMM                 10.13.2.248
default             0.0.0.0
procr               10.13.2.247




( 4 of 4 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

2. Enter the name and IP address for the C-LANs and LSPs.
3. Press **F3** (**Enter**) when complete.

Administering Network Regions

Before assigning an IP network region to a media gateway, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a particular media gateway with an S8300 LSP and an S8500 or S8700-series Server as the primary controller, there may be more than one network region. The media gateway is connected to the S8500 or S8700-series Server with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700-series port networks, though they may also have the same network region.

Note:

With an S8300 or an S8400 Server, there still may be a need for more than one network region, though the S8400 supports up to five media gateways and the S8300 supports up to 50 media gateways.

To configure IP network regions for a media gateway and CLAN board(s)

CAUTION:

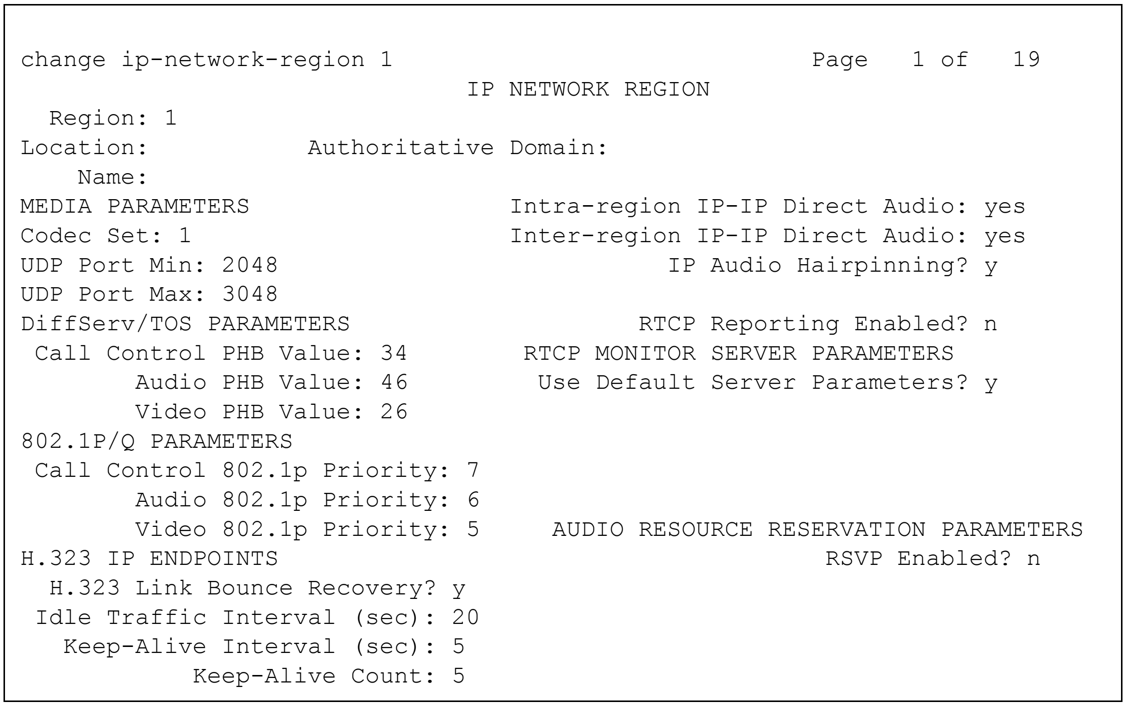
Configuring IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

1. On the SAT screen of the primary controller for a media gateway, type **`change ip-network-region`** ***`<network_region>`***

   where ***`<network_region>`*** is the region you will assign to the media gateway. This region number may or may not match the network region of the S8400, S8500, or S8700-series CLAN boards.

   The system displays the **IP Network Region** screen.

IP Network Region Screen



```
change ip-network-region 1                             Page   1 of   19
                               IP NETWORK REGION
  Region: 1
Location:           Authoritative Domain:
    Name:
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
Codec Set: 1                      Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                           IP Audio Hairpinning? y
UDP Port Max: 3048
DiffServ/TOS PARAMETERS                    RTCP Reporting Enabled? n
 Call Control PHB Value: 34        RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46         Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

2. Complete the fields as described in *Administering Network Connectivity on Avaya Aura™ Communication Manager,* 555-233-504*.*

Note:

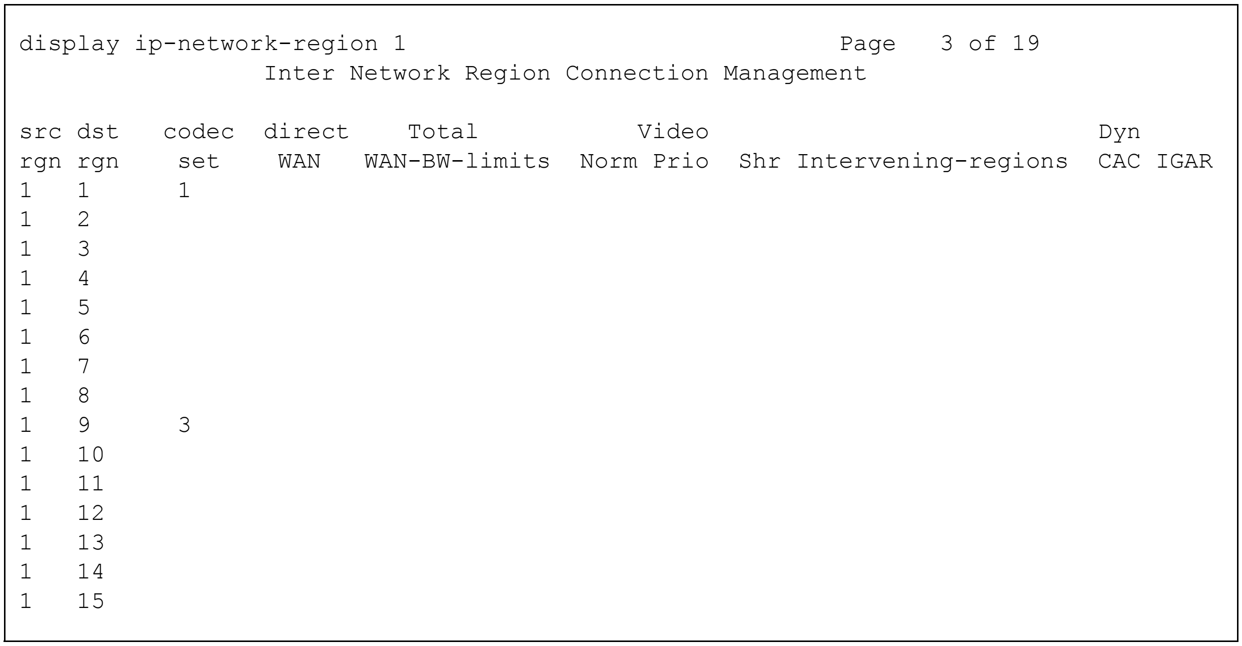
It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. If the network region of the media gateway (1 in this example) is different from that of the S8400, S8500, or S8700-series CLAN board(s), you must interconnect the two regions.

   Press **NextPage** twice to display page 3, of the **Inter Network Region Connection Management** screen.

   This screen shows the source region (1) and the first 15 destination network region numbers. (Pages 4–19 show destination regions 16–250).

IP Network Region Screen, Page 3



```
display ip-network-region 1                               Page   3 of 19
                 Inter Network Region Connection Management

src dst   codec  direct    Total           Video                          Dyn
rgn rgn    set    WAN   WAN-BW-limits  Norm Prio  Shr Intervening-regions  CAC IGAR
1   1      1
1   2
1   3
1   4
1   5
1   6
1   7
1   8
1   9      3
1   10
1   11
1   12
1   13
1   14
1   15
```

4. Type the number for the type of codec set (1–7) that the S8400, S8500, or S8700-series Server will use to interconnect the media gateways and the C-LAN board(s) in the row corresponding to the region of the C-LAN.

   In this example, the C-LAN is in region 9 and codec-set type 3 is to be used for the interconnection between region 1 and region 9. (In this example, codec type 1 is used for communication within region 1.)

   The SAT command, **list ip-codec-set**, lists the types of codecs available on this server.

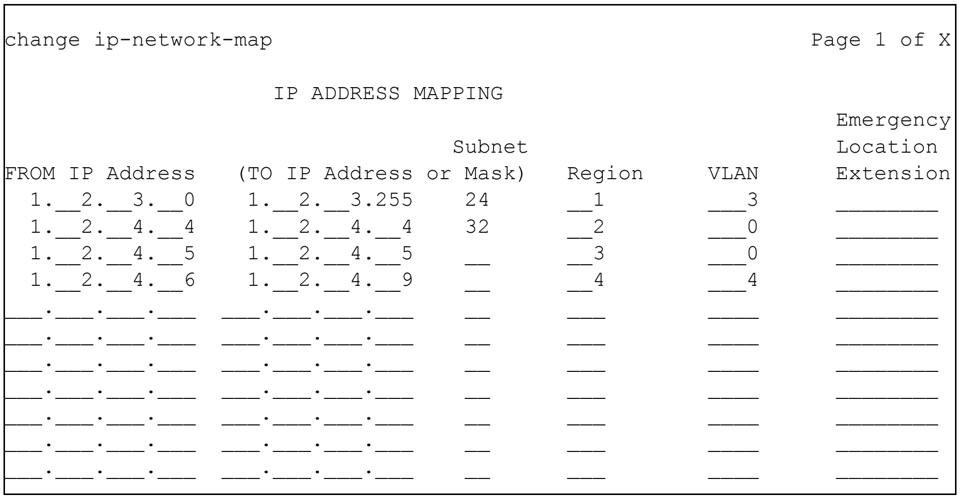
   For more detail about the Inter Network Region Connection Management form, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

5. Press **F3** (**Enter**) when complete.

Administering the IP address map

Administer the IP address map to assign IP phones and other IP endpoints to the same network region as the media gateway.

1. Type **`change ip-network-map`** and press **Enter** to display the **IP Address Mapping** screen.



```
change ip-network-map                                           Page 1 of X

                     IP ADDRESS MAPPING
                                                                  Emergency
                                   Subnet                         Location
FROM IP Address   (TO IP Address or Mask)   Region     VLAN       Extension
  1.__2.__3.__0    1.__2.__3.255    24      __1        ___3       ________
  1.__2.__4.__4    1.__2.__4.__4    32      __2        ___0       ________
  1.__2.__4.__5    1.__2.__4.__5    __      __3        ___0       ________
  1.__2.__4.__6    1.__2.__4.__9    __      __4        ___4       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
___.___.___.___  ___.___.___.___    __      ___        ____       ________
```

2. In the **FROM IP Address** and **TO IP Address** fields, enter a range of IP addresses for IP phones or other IP endpoints connected to the media gateway.
3. In the **Region** field, enter the network region to which the media gateway and its IP endpoints are to be assigned.
4. In the **VLAN** field, enter the VLAN number the IP endpoints should be a member of. Each network region should have its own VLAN number.
5. Enter an extension number in **Emergency Location Extension** field.

   Note:

   > For more detail about the IP Address Mapping form, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Administering IP Interfaces

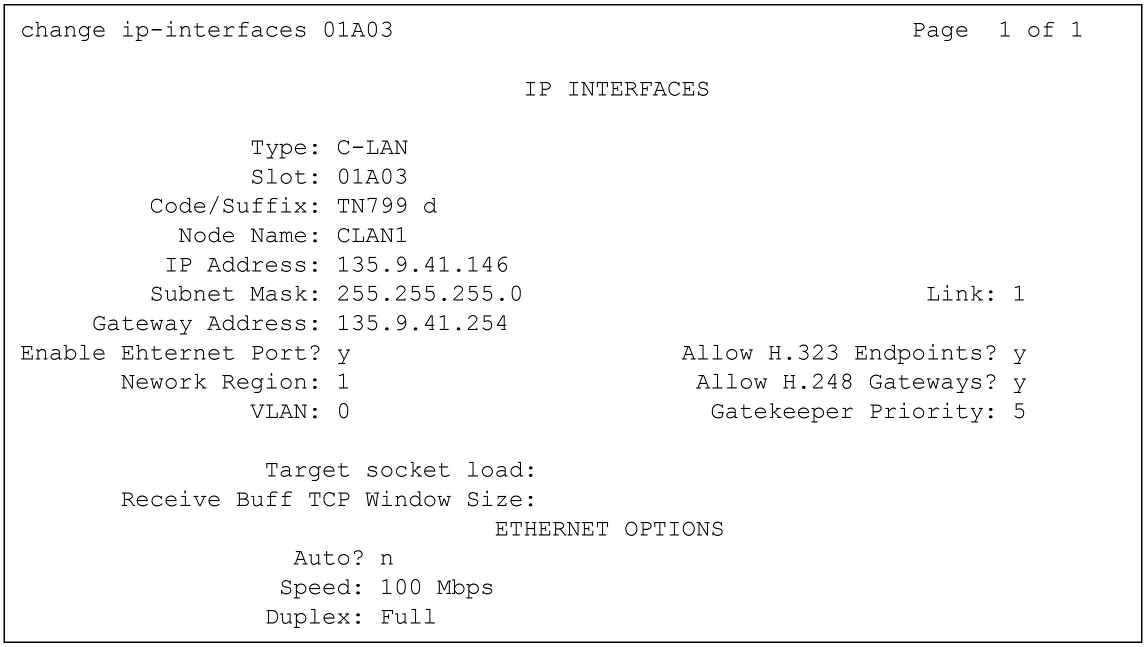
To define the IP interfaces of the S8400, S8500, or S8700-series port network CLAN boards

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Server installation.

1. Type **`change ip-interfaces`** ***`<slot location>`*** to open the **IP Interfaces** screen.

IP Interfaces Screen



```
change ip-interfaces 01A03                                         Page  1 of 1

                                   IP INTERFACES

                Type: C-LAN
                Slot: 01A03
         Code/Suffix: TN799 d
           Node Name: CLAN1
          IP Address: 135.9.41.146
         Subnet Mask: 255.255.255.0                           Link: 1
     Gateway Address: 135.9.41.254
Enable Ehternet Port? y                      Allow H.323 Endpoints? y
       Nework Region: 1                       Allow H.248 Gateways? y
                VLAN: 0                        Gatekeeper Priority: 5

                 Target socket load:
       Receive Buff TCP Window Size:
                                 ETHERNET OPTIONS
                   Auto? n
                  Speed: 100 Mbps
                 Duplex: Full
```

2. Complete the fields as described the in Table 8.

Table 8: IP interfaces field descriptions

Field	Conditions/Comments
Type	Either C-LAN.
Slot	The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799 for C-LAN.
	1 of 3

Table 8: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Node name	The unique node name for the IP interface. The node name here must already be administered on the **Node Names** screen.
IP Address	The IP address (on the customer LAN) of the C-LAN.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see “*Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504”*.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
Enable Ethernet Port?	The Ethernet port must be enabled (**y**) before it can be used. The port must be disabled (**n**) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
VLAN	The VLAN number assigned to the C-LAN, if any.
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Receive Buffer TCP Window Size	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.
Link	This display only field shows the unique number for the Ethernet link. The Ethernet link was assigned on the data module form.
Allow H.323 Endpoints	Enter ’y’ to allow H.323 endpoint connectivity on this CLAN. Enter ’n’ if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter ’y’ to allow H.248 gateway connectivity to this CLAN. Enter ’n’ if you do not want H.248 gateways to connect to this CLAN.
	2 of 3

Table 8: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to a yes on this form.
Auto?	Enter ’y’ or ’n’ to set auto-negotiation.
Speed	Enter 10 or 100 Mbps if **Auto** was set to no.
Duplex	Enter half or full if **Auto** was set to no.
	3 of 3

3. Close the screen.

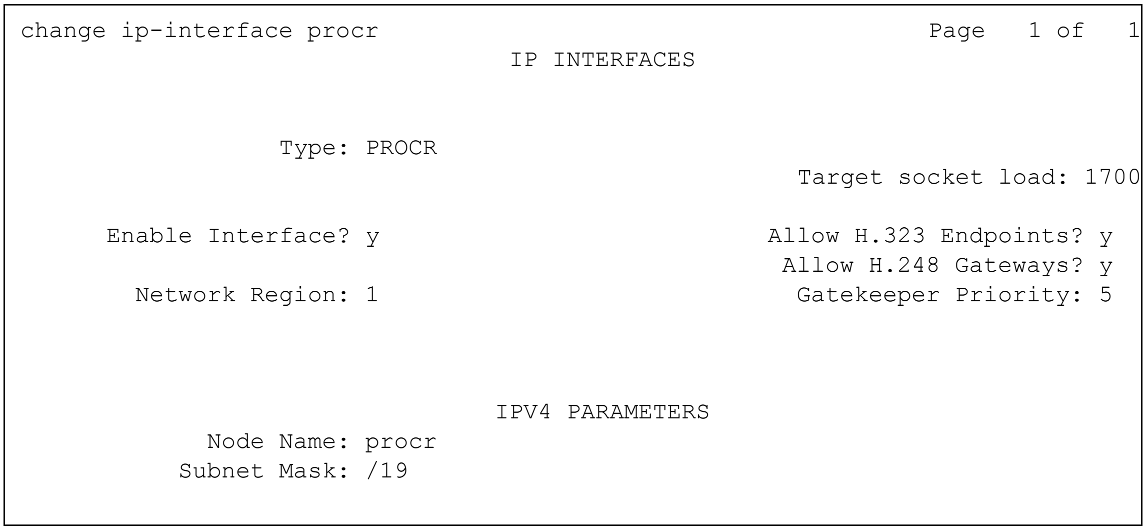
To define the IP interface of the S8400 or S8500 processor Ethernet port

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Server installation.

1. Type **`change ip-interfaces procr`** to open the **IP Interfaces** screen.

IP Interfaces Screen



```
change ip-interface procr                                    Page   1 of   1
                                  IP INTERFACES


                  Type: PROCR
                                                         Target socket load: 1700

      Enable Interface? y                              Allow H.323 Endpoints? y
                                                        Allow H.248 Gateways? y
        Network Region: 1                                Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /19
```

2. Complete the fields as described the in Table 9.

Table 9: IP interfaces field descriptions

Field	Conditions/Comments
Type	Display only. PROCR.
Node name	The unique node name for the IP interface. **procr** is the default node name. The node name here must already be administered on the **Node Names** screen.
IP Address	The IP address (on the customer LAN) of the Processor Ethernet.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see "*Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504"*.
Enable Ethernet?	The Ethernet port must be enabled (**y**) before it can be used. The port must be disabled (**n**) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
Target Socket Load	Enter the maximum number of sockets targeted for this interface. The default is 80% of the maximum of 2500 for an S8400 Server and 3500 for an S8500 or S8700-series Server. When all the IP interfaces within the same Gatekeeper Priority exceeds the target number that you allocate, the system continues to add sockets until the interface is at its maximum capacity.
Allow H.323 Endpoints	Enter 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to a yes on this form.

3. Close the screen.

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the survivable-processor screen, their status can be viewed with the **`list survivable-processor`** command.

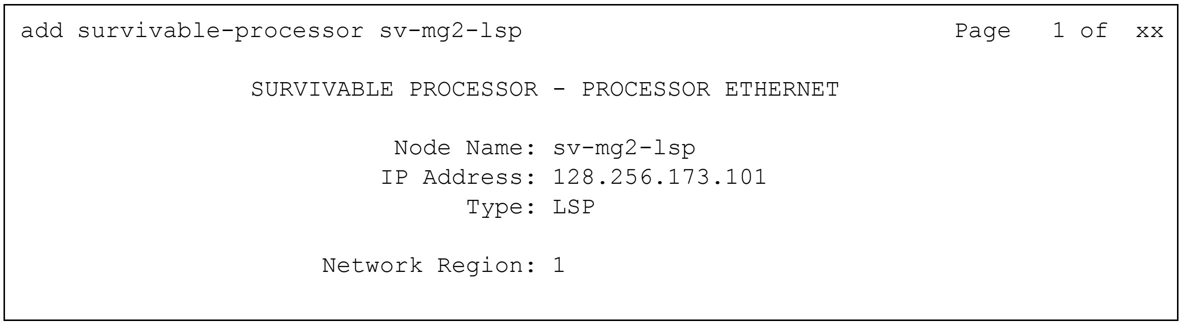
Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

1. At the SAT command line, type **`add survivable-processor`** ***<name>,*** where ***<name>*** is the LSP name from the **Node Names** screen.

   The **Survivable Processor** screen appears.

Figure 15: Add Local Survivable Processor screen



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

                SURVIVABLE PROCESSOR - PROCESSOR ETHERNET

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

                     Network Region: 1
```

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Node Name is a display-only field that shows the name used to identify this server. You enter node names through the IP Node Names screen.
4. IP Address is a display-only field that shows the IP address that corresponds to the node name you entered.
5. Enter a Processor Ethernet Network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support. Valid values can be from 1 to250. Enter the network region in which the PE interface of the LSP resides.

Assigning LSPs with Network Regions

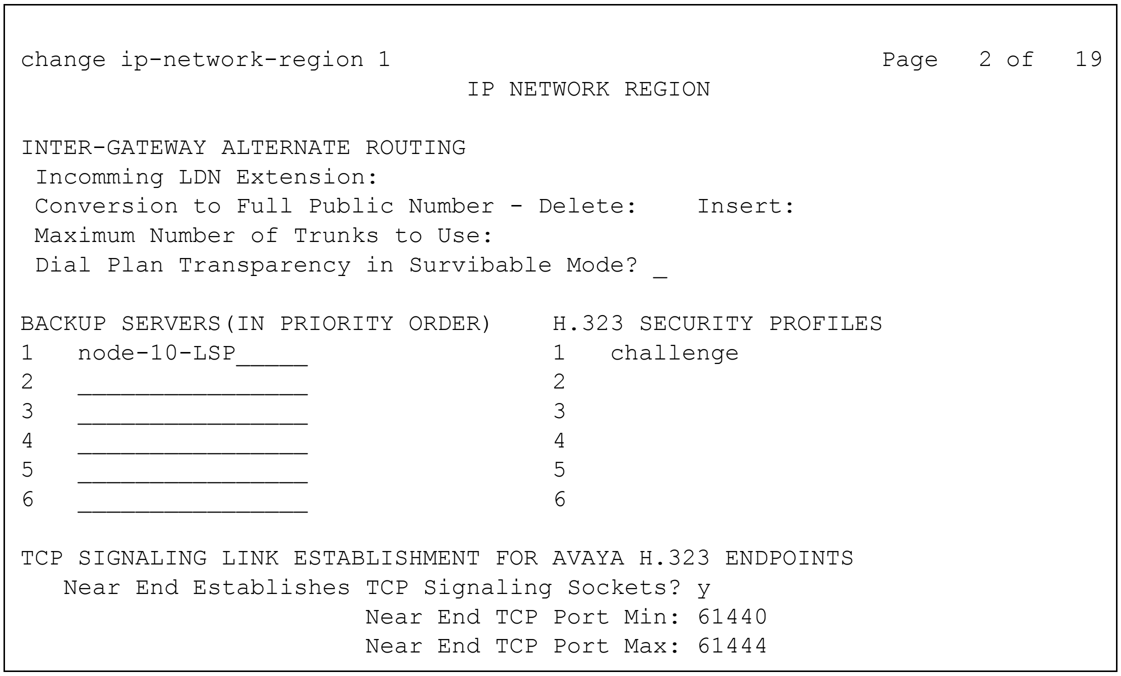
If the primary controller has LSPs, you can assign the LSPs to network regions. In the event of a network failure, IP telephones assigned to a network region will register with the LSPs assigned to that region.

This procedure assigns up to six LSPs to a network region.

To assign LSPs to a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2



```
change ip-network-region 1                                  Page   2 of   19
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING
 Incomming LDN Extension:
 Conversion to Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use:
 Dial Plan Transparency in Survibable Mode? _

BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES
1   node-10-LSP_____                 1   challenge
2   ________________                 2
3   ________________                 3
4   ________________                 4
5   ________________                 5
6   ________________                 6

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Sockets? y
                        Near End TCP Port Min: 61440
                        Near End TCP Port Max: 61444
```

2. Enter the names of up to six LSPs to be assigned to region 1.

   The LSP names must be the same as administered on the **Node Names** form.
3. Submit the form.
4. Repeat for each network region to which you want to assign LSPs.

Administering the Media Gateway with S8300 Server

To perform the procedures in this section, log in to the primary controller and open a SAT session.

⚠ **CAUTION:**

Before administering a media gateway, make sure that the gateway has been fully configured.

In this section, you will do the procedures:

- To add a media gateway
- To verify changes
- To enable announcements, if necessary

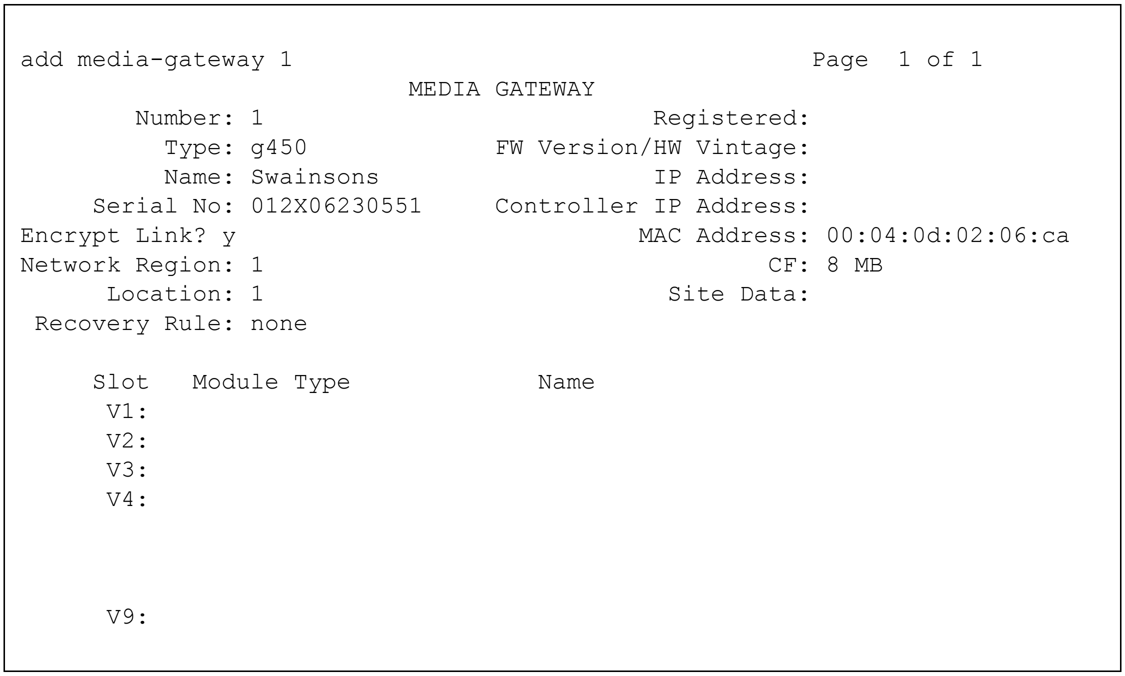
To add a media gateway

1. At the SAT prompt, type **`add media-gateway`** ***`<number>`***

   where ***`<number>`*** is the gateway number from 1 to *n*. (*n* is 50 for an S8300, 5 for an S8400, and 250 for an S8500 or S8700-series Server).

   The S8300 displays the **Media Gateway** screen.

Add media gateway Screen



```
add media-gateway 1                                    Page  1 of 1
                           MEDIA GATEWAY
        Number: 1                           Registered:
          Type: g450             FW Version/HW Vintage:
          Name: Swainsons                   IP Address:
     Serial No: 012X06230551     Controller IP Address:
Encrypt Link? y                            MAC Address: 00:04:0d:02:06:ca
Network Region: 1                                   CF: 8 MB
      Location: 1                            Site Data:
 Recovery Rule: none

     Slot   Module Type             Name
      V1:
      V2:
      V3:
      V4:



      V9:
```

2. Complete the **Name** field with the hostname assigned to the media gateway.
3. Complete the **Serial No** field with the serial number of the media gateway.

   You can obtain the serial number by typing the **`show system`** command at the MGP command line interface.

⚠ **CAUTION:**

> Be sure the serial number for the media gateway you enter in this procedure matches *exactly* the serial number displayed in the **`show system`** command. The serial number is case-sensitive, and if entered incorrectly, will prevent the S8300 Server from communicating with the media gateway.

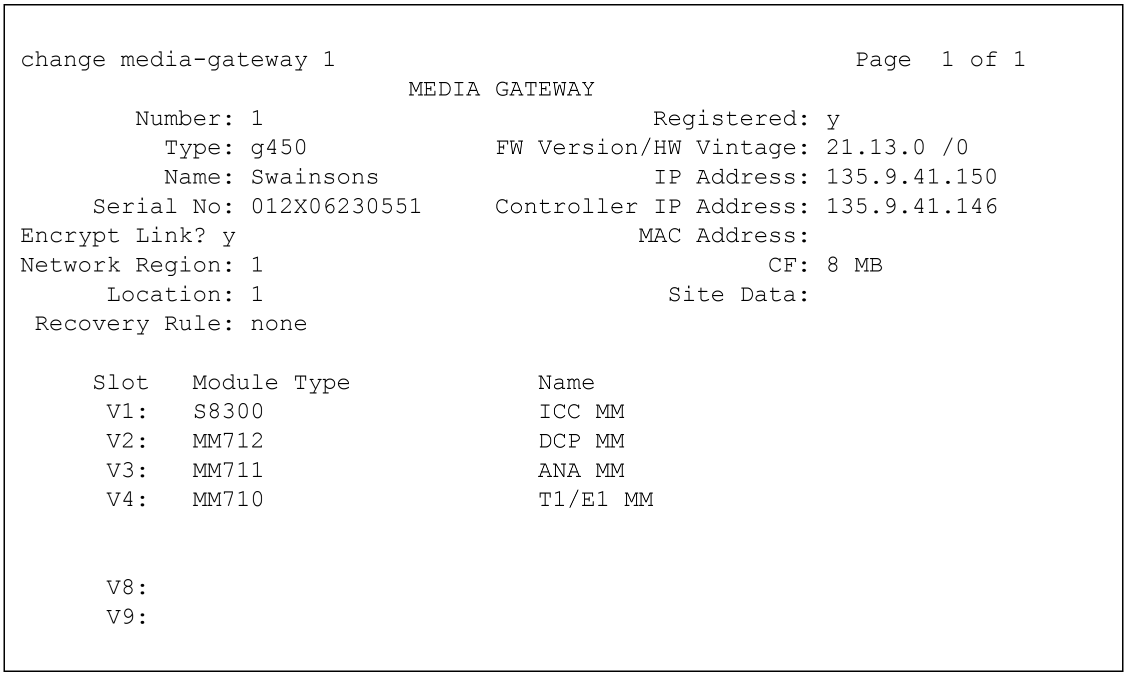
4. Complete the **Network Region** field with the value supplied in the planning documentation.
5. If specifically requested by the customer or your planning documents, type **gateway-announcements** in the V9 field.

   This field allows you to enable announcements on the media gateway. V9 is a virtual slot. There is no announcement board associated with it. The announcements for the media gateway are available in the media gateway firmware and are administered in the same way as announcements on the TN2501 circuit pack used on S8400, S8500, or S8700-series port networks.

   If there are multiple media gateways sharing announcements, then enable announcements on the media gateway whose trunks will receive the announcements most often.
6. Press **F3** (**Enter**) to save your changes.

   If properly administered, the media gateway should register with the primary controller within 1–2 minutes. The **IP Address**, **MAC Address**, and **Module Type** fields are populated automatically after the media gateway registers with the server.
7. Type **`display media-gateway n`**, where `n` is the media gateway number, to view the **Media Gateway** screen.

Media Gateway screen (after registration with primary controller)



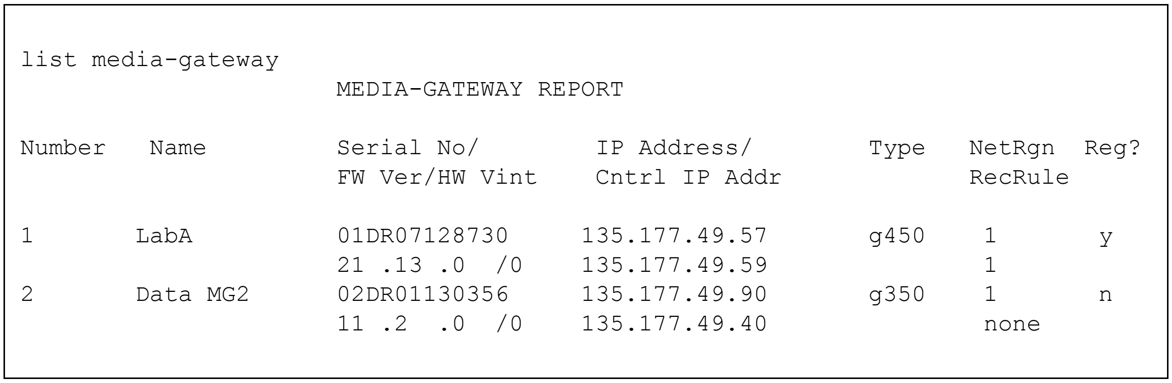
```
change media-gateway 1                                     Page  1 of 1
                          MEDIA GATEWAY
        Number: 1                        Registered: y
          Type: g450            FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                  IP Address: 135.9.41.150
     Serial No: 012X06230551     Controller IP Address: 135.9.41.146
Encrypt Link? y                           MAC Address:
Network Region: 1                                  CF: 8 MB
      Location: 1                           Site Data:
 Recovery Rule: none

     Slot   Module Type            Name
      V1:   S8300                  ICC MM
      V2:   MM712                  DCP MM
      V3:   MM711                  ANA MM
      V4:   MM710                  T1/E1 MM


      V8:
      V9:
```

The media modules installed in the media are listed next to their slot numbers. Verify that the media gateway has been successfully added.

To verify changes

1. At the SAT prompt, type **list media-gateway**.

Media-Gateway Report screen



```
list media-gateway
                      MEDIA-GATEWAY REPORT

Number   Name         Serial No/        IP Address/        Type   NetRgn  Reg?
                      FW Ver/HW Vint    Cntrl IP Addr             RecRule

1       LabA          01DR07128730     135.177.49.57       g450    1       y
                      21 .13 .0  /0    135.177.49.59               1
2       Data MG2      02DR01130356     135.177.49.90       g350    1       n
                      11 .2  .0  /0    135.177.49.40               none
```

2. Verify that the media gateway has registered.

   The y in the registered field signifies that the media gateway has registered. If the media gateway should become unregistered, the y will become an n, but the IP address will remain assigned to the media gateway. If the has never been registered, the IP Address field will be blank.

   If the media gateway fails to register, two common causes are:

- The serial number administered in the **Serial No** field on the change media-gateway form is incorrect. To check, log back into the media gateway and type **`show system`**. Check the serial number that appears.
- There is no IP connection between the media gateway and the S8300. To check, type **`show mgc`** and then **`ping mgp`** ***`<controller_address>`***.

To enable announcements, if necessary

1. *Only if specifically requested by the customer or your planning documents,* at the SAT prompt, type **`enable announcement-board`** ***`<gateway_number>`*** **`V9`**

   where ***`<gateway_number>`*** is the number of the media gateway you added.

   `V9` is the virtual slot (for example, ***`2V9`*** means media gateway number 2, slot V9.
2. Press **Enter** to enable announcements.

   The system displays the message,

   ```
   Command successfully completed
   ```

Saving Communication Manager translations

Note:

If the S8300 you are installing is an ***LSP***, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session and log in as *craft* (or *dadmin*).
2. If the S8300 you are installing is a primary controller, at the SAT prompt, type **`save translation all`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

If using CM Messaging, administer Communication Manager for CM Messaging

A number of administration tasks must be performed to allow CM Messaging to work. These tasks are explained in detail in *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration* guide.

⚠ **CAUTION:**

CM Messaging processes messages using the G.711 codec only. Therefore, ensure that a codec set exists that uses only the G.711 codec. Then, assign that codec set to a network region. And, finally, assign that network region to the CM Messaging signaling group that is linked to the CM Messaging trunk group.

Administering SES

Installing the SES license

If you enabled SES on the **Server (Maintenance)** Web page, you must install the SES license from the WebLM server that is located on an edge or a combined home/edge server:

1. On the **System Management Interface** main page, under the **Administration** menu, click **SIP Enablement Services**.

   The system displays the **Integrated Management SIP Server Management** screen.

2. Select **Server Configuration > License**.

   The **List Licenses** page displays.

3. Click **Access WebLM**.

   The **WebLM** application screen displays in a new window.

4. If this is the first time the application has run, you must log in with *admin* as the default login and *weblmadmin* as the default password, then change both the default login and password to the customer’s preferences for this account.

Note:

> If the WebLM server is on a different subnet than the server, you must change the URL in your browser to include the server's DNS name. When you mouse-over the WebLM link on the List Licenses page, the URL includes an IP address, for example, "https://12.34.56.78/WebLM/index.jsp/." Change the URL to "https://*server-name*/WebLM/index.jsp/," where *server-name* is the DNS name of the server on which you want to install the SES license.

5. Select **License Administration**.

   The authentication screen appears.

6. Login as *admin* and enter the password.

   After this initial login, the system prompts you to change the password.

7. Change the password.

   WebLM logs you out.

8. Log in again as *admin* with the newly-created password.

   The **Web License Manager (WebLM)** screen appears.

9. Select **Install License**.

   The **Install License** page displays.

10. Click **Browse** to navigate to the SES license that you want to install.

11. Click **Install**.

    If the license is valid, the system indicates that it was installed successfully; otherwise the process fails with a brief description.

    Note:

    > The license update for the home seats can take up to 15 minutes. Wait approximately 15 minutes before continuing with verifying the license installation (Step 12).

12. To verify the license installation go to the Integrated Management SIP Server Management **Top** page and select **Server Configuration > License**.

    The **List Licenses** page displays.

13. Ensure that the following three (3) licenses are listed in the **Name** column:

    - Edge Proxy
    - Basic Proxy
    - Home Seats

14. Click **Show** by the Edge Proxy listing.

    The **License Information** page displays.

15. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   1
    Acquired    1
    ```

16. Click **Show** by the Basic Proxy listing.

    The **License Information** page displays.

17. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   1
    Acquired    1
    ```

18. Click **Show** by the Home Seats listing.

    The **License Information** page displays.

19. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   XXX
    Acquired    XXX
    ```

    where `XXX` is the actual number of seats in the license.

20. Reboot the S8300 server:

    a. Click **Shutdown Server** under the Server heading.

    b. Select **Delayed Shutdown and Restart server after shutdown**.

    c. Click **Shutdown**.

    You will be logged off the server when it reboots. You can use ping to verify when the server is accessible again.

SES administration tasks

If you enabled SES, you must complete the following tasks to administer SES. For more information, see *Administration of SIP Enablement Services on the S8300 Server*.

1. Prepare Communication Manager.
2. Administer SIP trunks.
3. Administer call routing.
4. Administer SCCAN, if desired.

5. Administer Redirect Call Off-Net, if desired.
6. Complete the following SES Setup screens.
   - **Edit System Properties** screen, which you use to set up the SIP domain
   - **Add Host** screen, which you use to define the other servers for SES
   - **Edit Default User Profile** screen, which you use to enter location information to be assigned to each user on the local server
   - **Add Media Server** screen, which you use to define the S8300 as a host running Communication Manager
   - **Set up Master Administration** screen, which you use to define the server for storage of the main SES database
   - **WEbLM** screen, which you use to install the SES license.

Considerations for IP Phones Supported by a Local Survivable Processor

A DHCP server assigns IP addresses to IP endpoints dynamically. Avaya IP phones perform a DHCP discover request to receive an IP address, as well as receive parameters necessary to function correctly. These parameters include the location of the call control server, the location of the TFTP server, as well as the directory on the TFTP server from which the phone receives its upgrades.

When preparing a DHCP server to work with Avaya IP phones, there is an option that must be administered to allow the Avaya phone to receive the DHCP offer. This option is “site-specific-option-number” (sson) 176. Different DHCP servers allow for this administration in different ways, but the sson option must be mapped to 176. Then the option can be set up to send the information desired to the Avaya phones for the intended activity.

The sson option sends a string that includes the IP address of the Avaya Call Controller with which the phone will register (“MCIPADD=www.xxx.yyy.zzz”). In an S8400, S8500, or S8700-series system, this can be a CLAN address; in an S8400 or S8500, this can also be the IP address for the server’s port that is enabled for processor ethernet; in an S8300 system, this is the IP address of the S8300. Multiple addresses can be administered to allow for LSP failover. The second address in the MCIPADD list may be an IP address for a second CLAN board or an LSP. If a second CLAN board is used, then the third address must be the LSP, and any subsequent addresses should be alternate LSPs. Local LSPs should appear first in the list, with remote LSPs later in the list as possible back ups.

If an IP phone loses its connection to the primary controller, it will try to register with an LSP associated with its network region (as defined on page 3 of the IP Network Region form). However, if the phone resets, it looses this information and goes to the DHCP server for a controller. If the only controller in the MCIPADD list is the primary controller, and if the connection to the primary controller is down, the phone cannot register. Having an LSP in the MCIPADD list gives the IP phones an alternate controller in this situation.

Note:

It is strongly recommended that at least one LSP be administered in the MCIPADD list.

Also included in the sson option string is the “MCPORT=1719”. This is the port the phone will listen on for signalling traffic to the call controller. Next is the tftp server field. This field indicates to the phone where it is to receive firmware updates, along with the tftp directory field.

Note:

See *4600 Series IP Telephone LAN Administrator’s Guide*, 555-233-507, for information about IP Telephones.

All phones for which the DHCP server has an LSP as the second address in the MCIPADD list should be administered to be in the same network region. Or, if administered to be in different network regions, the network regions involved should be interconnected. Use the ip-network-map form on the primary controller to put the IP phones in the same network region. On the ip-network-map form, a range of IP addresses (or a subnet) can be specified to be in a single network region. Enter the IP address range, or subnet, that contains the IP addresses of the IP phones and enter the desired network region number for that address range. The same address range or subnet must then be administered on the DHCP server. If it is not desired that all the phones be in the same network region, the form “ip-network-region #” should be used to interconnect all the network regions that contain those phones.

Transition of Control from Primary Controller to LSP

When the network connection between the media gateway and the S8300, S8400, S8500, or S8700-series primary controller goes down, control of endpoints connected to the media gateway goes to the next point in the primary controller list, which will be either a second CLAN board (when used with the S8400, S8500, or S8700-series) or an LSP. At this point, the primary controller alarms to notify the customer and services personnel that the network connection between the primary controller and media gateway has problems. If control passes to the LSP, the LSP’s license allows it to support the media gateway endpoints for up to 30 days, within which the network problems should be resolved.

The customer may pass control back to the S8300, S8400, S8500, or S8700-series primary controller manually, by selecting **Shutdown this server** from the S8300 LSP web page (includes selecting the option to restart after shutdown), or a technician must run **`reset system 4`** from the SAT command line from the S8300 LSP. When the system reboots, the media gateway and its endpoints reregister with the primary controller.

The customer may also choose to administer Communication Manager on the System Parameters Media Gateway Automatic Recovery Rule screen, such that the primary controller accepts control back from the LSP as soon as possible, based on whether there are calls active or what time of day it is. See *Administering Avaya Aura™ Communication Manager,* 03-300509.

Split registration solution

The main server (Communication Manager) attempts to ensure the devices in a network region register to the LSP when administered to force telephones and gateways to active LSPs. This solution keeps branch-oriented operations intact with local trunk resources. LSPs turn active once a media gateway registers itself.

For example,

- A server failure activating LSPs disables all network regions served by the LSPs.

- The main server blocks future registrations of media gateways and telephones.
- The main server disables media gateways and telephones already registered with the LSPs.

Sequence of events

Administrator forces media gateways and telephones to active LSPs. The main server resets or the network fragments, causing a media gateway to unregister.

The following sequence of events occurs:

1. The media gateway registers to an LSP turning the status active.
2. The LSP reports the active status to the main server.
3. The main server unregisters all media gateways and telephones from itself. These network resources are administered for the LSP under the heading "BACKUP SERVERS" on the IP Network Region screen. These end points do not re-register on the main server.
4. The main server decides the time-day-window, scheduled to enable the endpoints to re-register or the enable mg-return command is executed.

Network Region type description

An LSP is administered as backup server for one or more network region forms. The LSP can have resources from one or more network regions (group). On implementing the split registration feature, the network regions status changes to auto-disable (ad). On reaching the Time-of-Day or executing enable mg-return command, the network regions are automatically enabled and the telephones and media gateways can register.

On executing the disable nr-registration command, network region status changes to manually disabled (rd). The administrator changes this status by executing the enable nr-registration command.

All network regions in a group are manually disabled (rd) when one or more network regions in the group have the status as rd. On activating an LSP in a group having manually disabled network regions, the auto disable (ad) code is activated. It searches for manually disabled (rd) status. Since some network regions in the group already have the manually disabled (rd) status, all network regions display the rd status.

Complete the Installation of the S8300 (if the Primary Controller)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test the endpoints
- Administer Communication Manager for trunks, features, networking, or other items required by the customer
- Complete the electrical installation
- Enable adjunct systems

Note:

Follow the existing process and procedures to register the S8300.

Reboot the server

To instate the foregoing administration and provisioning:

1. At the Maintenance Web Pages, select **Server > Shutdown** server.

   The **Shutdown This Server** page displays.
2. Select **Delayed Shutdown** and check the **Restart server after shutdown** box.
3. Click **Shutdown**.

Integrity check

After the server comes up verify the following:

1. Ping the IP address of the server and ensure connectivity.
2. On the **Server (Maintenance)** Web page, select **Server > Status Summary**.

   The **Status Summary Page** displays.
3. Verify the following:
   - **Mode** is **Active**.
   - **Server Hardware** is **okay**.

- **Processes** is **okay**.

4. Select **Server > Process Status**.

   The **Process Status** page displays.

5. In the Content section, select **Summary**.
6. In the Frequency section, select **Display once**.
7. Click **View**.

   The **View Process Status Results** page displays.

8. Verify that all processes are **UP**.

Updating Communication Manager Messaging, if installed

Stopping Communication Manager Messaging, if loading an Communication Manager Messaging update

After the upgrade is complete, perform the following post-upgrade tasks:

1. On the **Server (Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, under **Utilities**, select **Stop Messaging**.

   The **Stop Messaging Software** Web page is displayed.

3. Select the **Stop** button.

   The shutdown of the messaging server will begin when all users have logged off from Communication Manager Messaging or after three minutes have passed, whichever event comes first.Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing Communication Manager Messaging service pack (or RFU) files, if any

If Communication Manager Messaging is being used, a post-upgrade service pack for Communication Manager Messaging may be required. See the Communication Manager Messaging documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at http://support.avaya.com.

1. Select **Messaging Administration** from the main menu.
2. Under **Software Management,** select **Adv Software Installation**.

3. Select **Continue this operation without current system backup**.
4. Select the Communication Manager Messaging update package and click **Install Selected Packages**.

   Note:

   The system automatically prompts you to restart Communication Manager Messaging when the service pack has been installed. Therefore, if you restart Communication Manager Messaging at this time, you do *not* need to perform the following procedure, Starting Communication Manager Messaging.

Starting Communication Manager Messaging

⚠ **CAUTION:**

You do *not* need to perform this task if you restarted Communication Manager Messaging as a part of the installation of the Communication Manager Messaging service pack.

After the Communication Manager Messaging application has been updated, you must restart it using the following steps:

1. On the **Server** (**Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.
2. From the **Messaging Administration** Web page, under **Utilities**, select **Start Messaging**.

   The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.
3. When the message `End start_vm: voice messaging is now completely up` is displayed, close the Messaging Administration Web page and do the next procedure in this document.

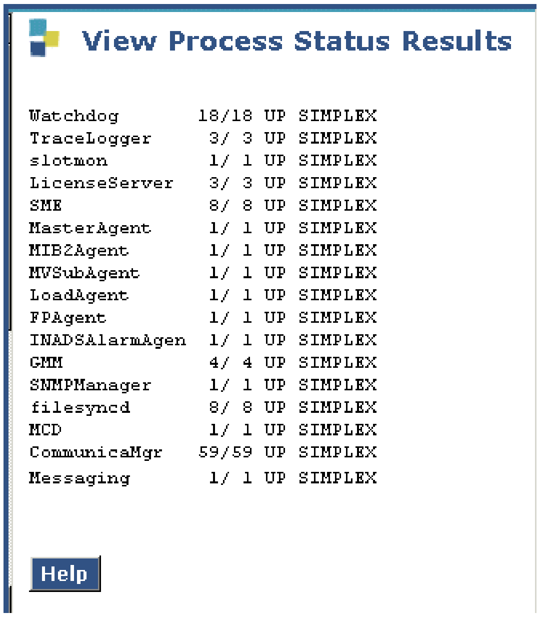
Verifying start up of Communication Manager Messaging

To verify operation of Communication Manager Messaging, perform the following steps:

1. On the **Server (Maintenance)** Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

   The **View Process Status Results** screen appears.

View Process Status Results screen



View Process Status Results

```
Watchdog        18/18 UP SIMPLEX
TraceLogger      3/ 3 UP SIMPLEX
slotmon          1/ 1 UP SIMPLEX
LicenseServer    3/ 3 UP SIMPLEX
SME              8/ 8 UP SIMPLEX
MasterAgent      1/ 1 UP SIMPLEX
MIB2Agent        1/ 1 UP SIMPLEX
MVSubAgent       1/ 1 UP SIMPLEX
LoadAgent        1/ 1 UP SIMPLEX
FPAgent          1/ 1 UP SIMPLEX
INADSAlarmAgen   1/ 1 UP SIMPLEX
GMM              4/ 4 UP SIMPLEX
SNMPManager      1/ 1 UP SIMPLEX
filesyncd        8/ 8 UP SIMPLEX
MCD              1/ 1 UP SIMPLEX
CommunicaMgr    59/59 UP SIMPLEX
Messaging        1/ 1 UP SIMPLEX
```

3. Make sure Messaging shows **UP**.

   The number of processes (59/59) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 58/59 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an Communication Manager Messaging sanity test:
   a. At the Linux command line, type **`/vs/bin/display`**.
   b. All states should be `Inserv` with an associated phone number.
   c. Retrieve the test message saved before the upgrade.
6. At the Linux command line, type **`/VM/bin/ss`**.
7. Verify that all Communication Manager Messaging processes are shown.

If Communication Manager Messaging fails to start after a new installation

If you have installed or upgraded Communication Manager Messaging and it does not start, you must ensure that an IP address has been provided for use with Communication Manager Messaging. To check for the IP address, you must use the **Configure Server** option on the Communication Manager System Management Interface.

On the Configure Interfaces screen, ensure that a valid IP address is present in the **Integrated Messaging** section**.**

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **`save translation all`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

Backing up system data

You can back up the S8300-Series Server data by:

- Backing up the system to compact flash media on page 198
- Backing up the system over the customer’s LAN on page 199

Backing up the system to compact flash media

S8300C Server allows back up using a compact flash card.

To back up the system to compact flash media

1. Plug the cable to the compact flash drive into a USB port on the S8300C Server.
2. Insert a 128-Mb compact flash media into the card reader or writer.
3. On the **Server (Maintenance)** Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.
4. In the Data Sets section select all of the following data sets:
   - If the S8300B, S8300C, or S8300D Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - If Communication Manager Messaging is installed on the S8300B, S8300C, or S8300D Server, select **Translations, Names and Messages**.

Note:

Depending on the customer's Communication Manager Messaging configuration, the back up size of the Communication Manager Messaging data set (**Translations, Names and Messages)** can be larger than the size of the compact flash drive (maximum size of the compact flash drive is 128 MB).

5. Select the Backup Method:
   - Local PC Card
6. Optionally, select **Format Compact Flash** to format a new card.

Note:

The compact flash card needs to be formatted only before the first use.

7. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

Backing up the system over the customer's LAN

To back up the data on an S8300 Server:

1. On the **Server (Maintenance)** Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.
2. In the Data Sets section select all of the following data sets:
   - If the S8300B, S8300C, or S8300D Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - If Communication Manager Messaging is installed on the S8300B, S8300C, or S8300D Server, select **Translations, Names and Messages**.
3. Select the Backup Method:
   - Network Device: enter the customer-supplied information for:
     - User Name

       You must enter a valid user name to enable the S8300 Server to log in to the FTP, SFTP, or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.
     - Password

       You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP site may have a different convention.

- Host Name

  Enter the DNS name or IP address of the FTP, SFTP, or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

- Directory

  Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. If you do not want to use the default directory, you must enter the full path from the ftp server root.

4. Click **Start Backup**.

   Wait for the message indicating that the backup was successful.

5. To check the status of the backup:

   a. Under **Data Backup/Restore**, click **Backup History**.

   b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

      When the backup is finished, the **Backup History Results** screen displays the following message:

   ```
   The final status for your backup job is shown below
   ```

   For each backup set, the following message is displayed if set was backed up successfully:

   ```
   BACKUP SUCCESSFUL
   ```

   ⚠ **Important:**
   When you do full back up, Communication Manager Messaging data is not backed up.

6. If Communication Manager Messaging is installed on the S8300A , S8300B, S8300C, or S8300D back up announcements:

   - Return to the **Backup Now** screen and uncheck all but **Announcements**.
   - Select the Backup Method (see Step 3 above).
   - Click **Start Backup**.

Complete the Installation Process (for an S8300 LSP)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test endpoints

This completes the installation of the media gateway with an S8300 LSP.

Final tasks

Perform the following tasks to complete the server installation:

1. On the **Sever (Maintenance)** Web Pages, select **Server > Status Summary** and check the overall health of the system.
2. Resolve any alarms (**Alarms > Current Alarms**).
3. Save translations (**Data Backup/Restore > Backup Now**).
4. Set backup schedules (**Data Backup/Restore > Schedule Backup**).
5. At the server command line type **`productid -p`** ***`product_id,`*** where ***`product_id`*** is the product ID you received from the customer or the ART tool.
6. Re-enable alarm origination:
   a. At the server command line type **`almenable -d b -s y`** and press **Enter**, where:
      - **`-d b`** sets the dialout option to both numbers
      - **`-s y`** enables sending SNMP traps.

   b. Type **`almenable`** without any options and press **Enter** to verify that alarm origination is enabled.
7. Logoff the system.

Chapter 4: Upgrading Communication Manager on an existing S8300B or S8300C Server

This chapter covers the methods and procedures to upgrade the software on an installed Avaya S8300B or S8300C Server from release 2.x, 3.x, or 4.x, 5.0, or 5.1 to release 5.2.

⚠ **Important:**

This chapter assumes that the currently installed S8300 is version B or C. The S8300B runs Communication Manager release 2.0 or greater. The S8300C runs Communication Manager release 4.0 or greater. If the currently installed S8300 is version A, follow the migration procedure in Chapter 7: Migrating an S8300 Server on page 351.

Upgrading Communication Manager on an S8300B or an S8300C to release 5.2

Select from any of the following methods:

- Software Update Manager
- Manage Software Web page

⚠ **Important:**

You cannot use the following tools to upgrade Communication Manager software to release 5.2:

- Avaya Installation Wizard
- Upgrade Tool

However, to upgrade to pre-5.2 release, you can use the Avaya Installation Wizard pre-5.2 release or the Upgrade Tool.

⚠ **Important:**

These procedures assume that you are upgrading an S8300 primary controller and/or an S8300 LSP.

⚠ **Important:**

The procedures to upgrade an S8300B or an S8300C Server using the Manage Software Web page are covered in Chapter 6: Manual upgrade of an existing S8300B or S8300C to Release 5.2 on page 287

⚠ **Important:**

If you are replacing an S8300A or S8300B with an S8300C or S8300D; or if you are replacing an S8300C with an S8300D use the procedures in Chapter 7: Migrating an S8300 Server on page 351.

Section 3: Manual procedures to install and upgrade an S8300 Server

This sections contains procedures to install or upgrade to Communication Manager release 5.2.

This section is organized into the following chapters:

- Chapter 5: Manual installation of an S8300 Server
- Chapter 6: Manual upgrade of an existing S8300B or S8300C to Release 5.2

Note:

Automated procedures to perform many of these tasks, using Avaya wizard tool can be found in Section 2: S8300 Server installation and upgrades.

Chapter 5: Manual installation of an S8300 Server

This chapter covers the manual procedures to install a media gateway with an Avaya S8300 Server. The S8300 can be configured as either the primary controller or as a local survivable processor (LSP).

The new S8300 normally ships ***without any software on its hard drive***. To install the software, you need to have an external USB CD-ROM drive.

The media gateway ships with the firmware installed on the processors and media modules. However, you may need to upgrade Communication Manager, media gateway firmware, and/or media module firmware if the latest available versions are not currently installed.

If the S8300 is configured as an LSP, the primary controller, running Communication Manager, can be either another S8300, or an S8400, S8500, or S8700-series Server.

Note:

> Procedures to install or upgrade an S8400, S8500, or S8700-series Server are not covered in this document. See *Documentation for Avaya Aura™ Communication Manager, Media Gateways and Servers*, which is on the Avaya Support web site (http://www.avaya.com/support) or on the CD, 03-300151.

The steps to install an S8300 configured as an LSP are the same as the steps to install an S8300 configured as the primary controller, with the following additional considerations:

- The version of Communication Manager on the LSP must be the same as, or later than, the version running on the primary controller.
- For an LSP, you administer Communication Manager translations on the primary controller, *not* on the LSP. The primary controller then copies the translations to the LSP.
- An LSP *cannot* have SIP Enablement Services (SES) enabled.
- An LSP must be configured as XL if the primary controller is an S8720 Server in an XL configuration or an S8730 Server. Administer this option on the Configure Server — Configure LSP Web page.

Installation Overview

About software and firmware files

A new S8300 Server comes with a blank hard drive. The media gateway components should have current releases of firmware installed. It may be necessary to install a service pack on the S8300 after installing the Communication Manager software, and/or to upgrade the media gateway and media module firmware.

Communication Manager software is distributed on a CD-ROM that you take to the site. Additional files that may be needed are the most recent versions of the software service pack file and media gateway firmware files. You may need to obtain these files from the Avaya Support web site.

About access to the Communication Manager software distribution CD

The Communication Manager software distribution CD that you take to the customer site contains the files required to install release 5.2 and other files. Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate.

This chapter describes the upgrade procedure using the CD-ROM drive as source of the software.

About SIP Enablement Services and Communication Manager Messaging software

SIP Enablement Services (SES) and Communication Manager Messaging software is also stored on the Communication Manager software distribution CD-ROM.

SES software is automatically installed on the S8300 Server when you install Communication Manager. For SES to be administered and operational, you must enable SES software and install an SES-specific license after the software is installed.

Communication Manager Messaging software is optionally installed on the S8300 Server when you install Communication Manager. If the customer does not want to use Communication Manager Messaging, do not install Communication Manager Messaging software.

CAUTION:

You have the choice to disable Communication Manager Messaging software after you install the messaging software with Communication Manager. If you did not install CM Messaging software you need to reinstall Communication Manager, along with the Communication Manager Messaging software. You normally can perform this reinstallation of software by reusing the software previously copied onto the S8300 Server. This software is stored on the server and is accessible from the Manage Software Web pages. In this case, you run an upgrade of the server reusing the same software and selecting Communication Manager Messaging for installation.

Tasks to install the S8300 and the media gateway

Before going to the customer site

- Obtaining a USB DVD or CD-ROM drive on page 211
- Obtaining information that the project manager provides on page 211
- Obtaining the serial number of the media gateway, if necessary on page 212
- Checking for an FTP/SCP/SFTP server or compact flash for backing up data on page 212
- Obtaining service pack files, if needed on page 212
- Obtaining service pack and language files for Communication Manager Messaging, if necessary on page 214
- Completing the RFA process (Obtaining license and authentication files) on page 215
- Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary on page 216

Install the S8300

- Inserting the S8300 on page 218
- Accessing the S8300 on page 219
- Setting telnet parameters on page 220
- Installing the Communication Manager software on page 220
- Verifying software version on page 221
- Copying files to the S8300 hard drive on page 222
- Downloading optional language files, if needed on page 223
- Verifying the Time, Date, and Time Zone on page 223
- Creating a super-user login on the primary controller on page 224

- Configuring the S8300 on page 226
- Providing the keys.install file (If necessary) on page 238
- Installing the Communication Manager license on page 239
- If the server is an LSP, stop and start Communication Manager on page 241
- Installing security files, Communication Manager service packs and SES service packs, if any on page 242
- Saving translations on page 243
- Enabling SIP Enablement Services, if desired on page 243

Configuring and Installing firmware on a Media Gateway

Administer an S8300 primary controller

- Assigning Node Names and IP Addresses for the LSPs on page 247
- Administering Network Regions on page 247
- Associating LSPs with Network Regions on page 249
- Administering the IP address map on page 250
- Administering IP Interfaces on page 250
- Identifying LSPs to the S8300 primary controller on page 251

Administer an S8400, S8500, or S8700-series primary controller

- Assigning Node Names and IP Addresses for the C-LANs and LSPs on page 254
- Administering Network Regions on page 254
- Administering the IP address map on page 258
- Administering the IP address map on page 258
- Administering IP Interfaces on page 258
- Identifying the Survivable Processor on the primary controller on page 262

Administer the media gateway

- Administering the Media Gateway on page 264

Administer Integrated Messaging

- If using Communication Manager Messaging, administer Communication Manager for Integrated Messaging on page 268

Administer SES software

- Installing the SES license on page 269
- SES administration tasks on page 271

IP phones considerations

- Considerations for IP Phones Supported by a Local Survivable Processor on page 273

Transition from Primary Controller to LSP

- Transition of Control from Primary Controller to LSP on page 274

Set up alarming

- Configuring the primary server to report alarms to a services support agency on page 276
- Configuring the media gateway to send its traps to a network management system (NMS) on page 277

Complete the installation of the S8300 (if the primary controller

- Reboot the server on page 278
- Integrity check on page 278
- Updating Communication Manager Messaging, if installed on page 279
- Backing up system data on page 282

Complete the installation of the S8300 (for an LSP)

- Complete the Installation Process (for an S8300 LSP) on page 284

Final Tasks

- Final tasks on page 285

Before Going to the Customer Site

The procedures in this section should be completed before going to the customer site or before starting a remote installation.

Obtaining a USB DVD or CD-ROM drive

Installing Communication Manager on an S8300 requires remastering the S8300 hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB DVD or CD-ROM drive. Therefore, you must have a USB DVD or CD-ROM drive at the site.

Obtaining information that the project manager provides

Ask the project manager for the information needed to prepare for this installation.

Obtaining the serial number of the media gateway, if necessary

For a new installation of a media gateway with an S8300, you need the serial number of the media gateway in order to complete the creation of the customer's license file on the http://rfa.avaya.com web site. To get this number, look for the serial number sticker on the back of the media gateway chassis. If the unit is delivered directly to the customer and you will not have phone or LAN line access from the customer site to access the rfa.avaya.com web site, this task will require a preliminary trip to the customer site.

Checking for an FTP/SCP/SFTP server or compact flash for backing up data

During the installation and upgrade procedures, you can back up the system data to an FTP Server, or to a USB Compact Flash drive. You use a server on the customer's LAN for backups. You can back up using an SCP or SFTP Server only with Communication Manager release 3.1 or later.

- Check with your project manager or the customer for the following information about the FTP, SFTP, or SCP server.
  - Login ID and password
  - IP address
  - Directory path on the FTP Server

⚠ **Important:**
Before going to the customer site, make sure that you can use either a customer server for backups or a compact flash card.

Obtaining service pack files, if needed

If one or more service packs are required for this installation or upgrade procedure, and the service pack files are not on your software CD, download the service pack files from the Avaya Support web site to your laptop.

Service packs may or may not be needed, depending on the release of Communication Manager. For both new installations and upgrades, you may need to install a service pack after the installation.

To download a service pack

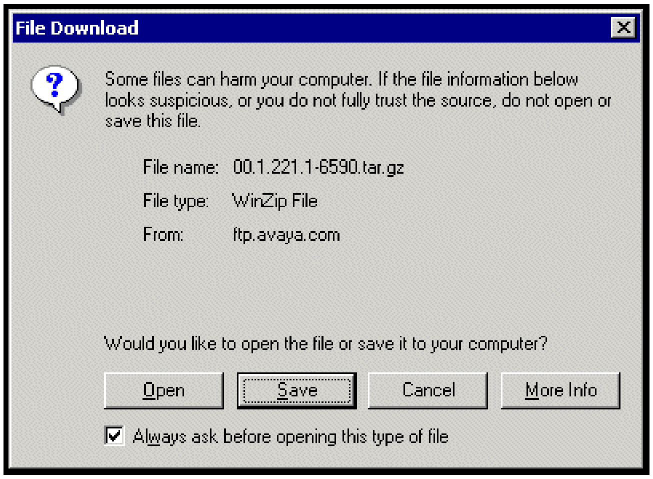
1. On your laptop, create a directory to store the file (for example, c:\S8300download).

2. Connect to the LAN using a browser on your laptop or the customer's PC and access http://www.avaya.com/support on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At the Avaya support site, select the following links:
   a. **Find documentation and downloads by product name**
   b. **S8300 Server**
   c. **Downloads**
   d. **Software downloads**
4. In the **Software Downloads** list, click the link for the appropriate Communication Manager release (for example, **Avaya Communication Manager Software Updates for 5.0**).
5. Scroll down the page to find a link called **Latest Avaya Communication Manager *x.x.x* Software Update** (where ***x.x.x*** is the release number).

   After this link, there should be a link starting with "**PCN**: "Click on this link to read about the release and software load to which this service pack applies.
6. Click **Latest Avaya Communication Manager *x.x.x* Software Update** (where ***x.x.x*** is the release that is currently running on the S8300).

   The File Download window appears.

File download window



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: 00.1.221.1-6590.tar.gz

File type: WinZip File

From: ftp.avaya.com

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

7. Click the **Save** button and browse to the directory on your laptop in which you want the file saved.

Obtaining service pack and language files for Communication Manager Messaging, if necessary

If Communication Manager Messaging will be installed, determine whether a service pack is needed and/or optional languages are used. If so, obtain the data files.

Obtaining an Communication Manager Messaging service pack file

If an Communication Manager Messaging service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an Communication Manager Messaging service pack file

1. On the Avaya Support Web site, click **Find Documentation and Downloads by Product Name**.
2. Under the letter "C", select **Communication Manager Messaging** application.
3. Click **Downloads**.

   To download the Communication Manager Messaging patch software:
4. Click **Communication Manager Messaging Application Patches**.
5. Click the service pack file name for this release.

   For example, **C6072rf+b.rpm**.

   > ⚠ **Important:**
   > While downloading the file it is possible that the Internet Explorer browser adds an extra character in the file name. Ensure that there are no extra characters in the file name before you save the file.
6. Click **Save** and browse to the location on your laptop where you want to save the file.

Obtaining Optional language files

Optional languages are any language other than English (***us-eng*** or ***us-tdd)***. If optional languages are used with this Communication Manager Messaging, you must download the appropriate language files from a language CD after the upgrade. The customer should have the language CD(s) at the site. If not, you need to obtain the appropriate language CD(s) and take them to the site.

Obtaining Ethernet interface IP address and subnet mask

If Communication Manager Messaging is to be installed, you must obtain an IP address and subnet mask to be used for the Ethernet interface for the H.323 integration. The subnet mask must be the same as that used for the S300 Server (control network), and is entered on the Configure Server Web screen when you configure the S8300.

Completing the RFA process (Obtaining license and authentication files)

Every S8300 Server and local survivable processor (LSP) requires a current and correct version of a license file in order to provide the expected call-processing service.

The Communication Manager license file specifies the features and services that are available on the S8300 Server, such as the number of ports purchased. The license file contains a software version number, hardware serial number, expiration date, and feature mask. The license file is reinstalled to add or remove call-processing features. New license files may be required when upgrade software is installed.

If the customer requires SES, you must acquire and install a separate SIP Enablement Services (SES) license file. You install the SES license as part of SES administrations, which you do after you install Communication Manager.

The Avaya password or authentication file contains the logins and passwords to access the S8300 Server. This file is updated regularly by Avaya services personnel, if the customer has a maintenance contract. All access to Communication Manager from any login is blocked unless a valid authentication file is present on the S8300 Server.

A new license file and the Avaya authentication file may be installed independently of each other or any other server upgrades.

Downloading license file and password file for an LSP

The license file for a S8300 configured as a Local Survivable Processor must have a feature set that is equal to or greater than the primary controller. The primary controller can be any of the following servers; S8300, S8400, S8500, S8700, S8710, S8720, or S8730 Server. This is necessary so that if control passes to the LSP, it can support the same level of call processing as that of the primary controller.

Additionally, the LSP must have a version of Communication Manager that is the same as, or later than, that of the primary controller.

Note:

The license file requirements of the LSP should be identified in your planning documentation.

To download the license and password files to your laptop

Tip:

Additional documentation on creating license files can be found on the RFA web site: http://rfa.avaya.com.

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and password files (for example, C:\licenses).
2. Access the Internet from your laptop and go to the Remote Feature Activation web site, http://rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and password files for the customer.
4. Check that the license and password files are complete. You might need to add the serial number of the customer's media gateway.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and password files to your laptop.

Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary

This step is necessary only if the configuration of the customer’s INADS alarming modem has changed.

Note:

ART tool is available to Avaya associates and a few Business Partners. **Business Partners** who do not have access to the ART tool must call 800-295-0099.

The ART tool is a software tool that generates an IP address for a customer’s INADS alarming modem. This IP address is required for configuring the S8300’s modem for alarming.

Note:

You must generate a license and authentication file before you use the ART tool. Also, the ART process is available *only* to Avaya personnel. You need an ART login ID and password, which you can set up at the ART web site. Non-Avaya personnel must contact their service support or customer care center for INADS addresses, if required.

To run the ART

1. Access the ART web site on your laptop at http://art.dr.avaya.com.
2. Select **Administer S8x00 Server products for installation script**.
   a. Log in.
   b. Enter the customer information.
   c. Select **Installation Script**.

d. Click **Start Installation script & IP Addr Admin**.

A script file is created and downloaded or emailed to you.

3. You can use the installation script to set up an IP address and other alarming parameters automatically.

Obtaining the static *craft* password (Avaya technicians only)

After installing new software and a new Authentication file, you will need to use a static craft password to access the customer's system. This static password will enable you to log in to the S8300 with a direct connection to the Services port without the ASG challenge/response. To obtain the static password, call the ASG Conversant number, 800-248-1234 or 720-444-5557 and follow the prompts to get the password. In addition to your credentials, you will need to enter the customer's Product ID or the FL or IL number.

Business Partners must use the *dadmin* password after the installation. Call 877-295-0099 for more information.

Install the S8300

Inserting the S8300

You must connect a USB CD/DVD-ROM drive to the S8300 server *before* you completely seat the S8300 server in the slot. Use one of the following external USB CD/DVD-ROM drives:

- Avaya approved Panasonic Digistor 73082 or 73322 (Comcode: 700406267):
  - The switch must be turned to the ON position.
  - Instead of AC power, the Panasonic Digistor uses a Lithium ION battery for additional power. The CD/DVD-ROM draws more power than the USB port can supply. The additional power required is supplied by the Lithium ION battery. If the Lithium ION battery is depleted, a red LED displays and a failed to mount CD-ROM message appears. You can charge the Lithium ION battery by plugging the CD-ROM drive in a USB port for approximately 30 minutes. The Lithium ION battery charges faster if the ON/OFF switch is set to OFF.

  Note:

  The functionality of the Lithium ION battery supplying the extra power that the CD/DVD-ROM needs is only applicable for the original CD/DVD-ROM.

- Addonics (Model: AEPDVRWII824) (not available through Avaya):
  - Requires AC power to operate.
  - You must have the switch set to External.
- TEAC (end of sale) (Comcode: 700289580)

⚠ **CAUTION:**

Be sure to wear a properly grounded ESD wrist strap when handling the S8300 Server. Place all components on a grounded, static-free surface when working on them. When picking up the hard drive, be sure to hold it only on the edges.

To insert the S8300

1. Connect the USB DVD/CD-ROM drive to the S8300 as follows:
   a. Place the CD/DVD-ROM drive on a surface within 5 degrees of level.
   b. If you are using an Addonics drive, plug one end of the CD/DVD-ROM power cord into the drive and plug the other end of the cord into an electrical outlet.
   c. Set the power switch to **EXT** (Addonics drive) or to **ON** (Panasonic drive). The TEAC drive does not have a switch.

d. Connect the USB cable to one of the USB ports on the faceplate of the server and the other end of the USB cable to the CD/DVD-ROM drive.

2. Insert the Communication Manager Software CD-ROM into the external CD/DVD-ROM drive.

   ⚠ **CAUTION:**

   Verify AC power connection to the laptop. Do not attempt to remaster the S8300 using only the laptop's battery power.

3. Push the server back into the appropriate slot depending on the media gateway used with S8300 Sever. For example, for an S8300 Server in a specific media gateway, insert the server in slot V1 guide until the front of the S8300 Server aligns with the front faceplate of the media gateway.

4. Secure the S8300 faceplate with the thumb screws.

   Tighten the thumb screws with a screw driver.

   Note:

   Unplug any external Compact Flash drive that might be connected to the S8300 USB ports. The S8300 tries to read any media connected to a USB port. The S8300 should only read the media on the CD-RW/DVD drive.

5. Power up the media gateway by plugging in the power cord.

6. Connect the laptop to the Services port on the faceplate of the S8300.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See Laptop configuration for direct connection to the services port on page 31.

You will use SSH and the Maintenance Web Interface to perform the procedures. See the following:

- Accessing the server's command line interface with SSH on page 44
- Logging in to the S8300 Web Interface from your laptop on page 46

Note:

Communication Manager has telnet turned off by default. Therefore, telnet is not available after remastering of the hard drive is complete during an initial server installation. However, if the customer later chooses to enable telnet, you may be able to use telnet to access the server's command line interface.

See About connection and login methods on page 31 for details on how physically to connect and log into the S8300 Server.

Setting telnet parameters

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 interprets this as two key presses. You need to correct this before you telnet to the server.

Note:

This procedure is done entirely on your laptop, not on the S8300.

To set telnet parameters

1. Click **Start > Run** to open the Run dialog box.
2. Type `telnet` and press **Enter** to open a Microsoft Telnet session.
3. Type `unset crlf` and press **Enter**.
4. Type `display` and press **Enter** to confirm that either `Sending only CR` or `Line feed mode--causes the return key to send CR` displays.
5. Close the window by clicking on the **X** in the upper-right corner.

This resets your Microsoft telnet defaults and does not need to be done each time you use Telnet.

Installing the Communication Manager software

To do before you start the installation

1. Verify that the S8300 is inserted in the appropriate slot of the media gateway (slot V1.
2. Verify good AC power connections to the media gateway.
3. Avaya recommends using a UPS backup for S8300 Servers.

   If a UPS is present, make sure the media gateway is plugged into the UPS.
4. Verify that all Ethernet connections are secure, to ensure the file transfer process is not interrupted.

To install the software (Communication Manager and optionally, Communication Manager Messaging) on the server:

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter.**
3. If the DVD/CD drive was not attached to a USB port when the server booted up, you will not see any activity on the screen. In this case perform the following:

   a. Press the Shut Down button on the server.

b. When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port.

c. Unseat and reseat the S8300C in its slot.

Tip:

To navigate the installation 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.

4. Select **Install** and press **Enter**.

   The **Select Release Version** screen appears.

5. Select the appropriate release version then select **OK** and press **Enter**.

   The **Select Messaging Option** screen appears.

   Note:

   Communication Manager Messaging is optionally installed on the server when you install Communication Manager.

6. Select from one of the following:

   1. CM Only <No Messaging>
   2. CMM <Embedded Messaging>

   The following processes are initiated:

   - The server's hard drive and internal Compact Flash are partitioned and reformatted.
   - The Linux operating system is installed.
   - Once the drive is properly configured, Communication Manager software is installed, if you select CMM <Embedded Messaging> and the progress reported.
   - If elected, Communication Manager Messaging is installed.

   The process takes about 30 minutes. When the server is ready to reboot, the CD drive door opens or the CD is ejected, and a reminderto check the Avaya Support Site (http://support.avaya.com/downloads) for the latest software and firmware updates displays.

   The reboot takes 1-3 minutes without Communication Manager Messaging and 3-6 minutes if it is present.

7. At your laptop click **Start > Run** to open the **Run** dialog box.

8. Type `ping -t 192.11.13.6` and press **Enter**.

9. Wait for the reply from the server to ensure connectivity to it.

Verifying software version

To verify the software version that you just installed:

1. Visit http://192.11.13.6.

2. On the Communication Manager Server Management Interface Web page, under the **Administration** menu, click **Server (Maintenance)**.
3. Select **Server > Software Version**.

   The **Software Version** page appears.
4. Verify that the server is running Release 5.2 software. The beginning of the **Report as:** string should show **R015x.02**.
5. Verify that the DVD/CD-ROM drive opened at the end of the software installation.
6. Disconnect the DVD/CD-ROM drive from the server's USB port.

Copying files to the S8300 hard drive

During reformatting of the hard drive, a new directory, ***/var/home/ftp/pub***, is created.

You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Communication Manager service pack
- License file (for Communication Manager, and optionally, for SES)
- Avaya authentication file
- New firmware files
- Security files
- Communication Manager Messaging service packs or RFUs

To copy files to the S8300 hard drive

1. Select **Miscellaneous > Download Files**.

   The **Download Files** page displays.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** to open the **Choose File** window to navigate to the files you want to download.
4. Select the file(s) to download.

   Note:

   If you need to download an IP telephone firmware file, download this file last with **Install this file on the local server** checked. The files are copied to the .../tftpboot directory, the IP telephone Web page is reinstated, and the firmware restored at the next reboot.

Note:

To manually FTP files from your laptop to */var/home/ftp/pub*, you must change the directory to *pub* (type **`cd pub`**) after starting FTP and logging in.

5. Click **Download** to copy the files to the server.

   The transfer is complete when the following message appears:

   ```
   Files have been successfully downloaded to the server
   ```

   ⚠ **Important:**

   Remove the Communication Manager software distribution CD from the CD drive.

Downloading optional language files, if needed

If the optional language files are needed, copy the files from the language CD to */var/home/ftp/pub*.

To download optional language files

1. Insert the optional language CD in your laptop’s CD-ROM drive.
2. In the Maintenance Web Interface, under Miscellaneous, select **Download Files**.
3. Select the **Files to download from the machine I’m using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click **Download**.

   When the transfer is complete, the following message appears:

   ```
   Files have been successfully downloaded to the server
   ```

6. If more than four optional language files need to be downloaded, repeat this procedure.

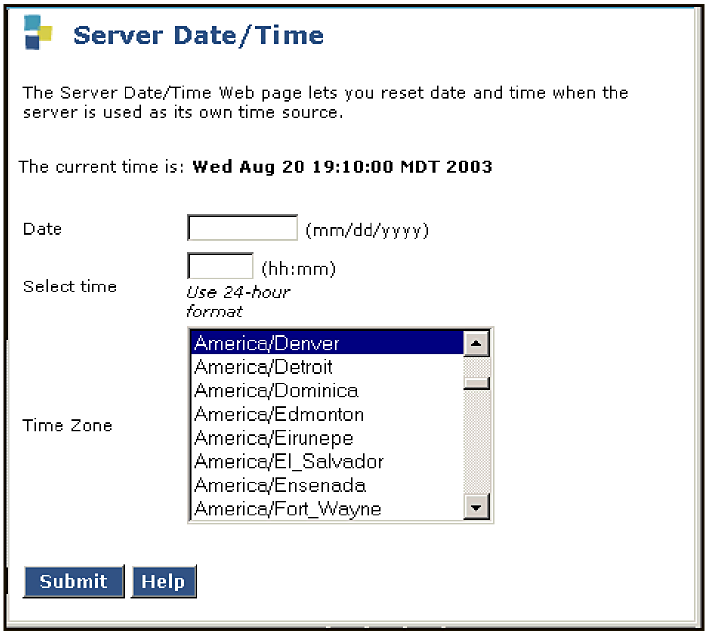
Copies of the optional language files are now in the */var/home/ftp/pub* directory and will be automatically installed during the upgrade process.

Verifying the Time, Date, and Time Zone

To verify the Time, Date, and Time Zone:

1. Under Server click **Server Date/Time**.

Server Date/Time Window



Server Date/Time

The Server Date/Time Web page lets you reset date and time when the server is used as its own time source.

The current time is: **Wed Aug 20 19:10:00 MDT 2003**

2. Verify or set the S8300 Server's time close enough to the NTS's time, date, and time zone that synchronization can occur (within 5 minutes).

   Note:

   > If you are configuring an LSP, the date and time must match the time zone of the primary controller.

3. If you set the time, date, or time zone, you must reboot the server:

   a. Click **Shutdown Server** under the Server heading.

   b. Select **Delayed Shutdown and Restart server after shutdown**.

   c. Click **Shutdown**.

   You will be logged off the server when it reboots. You can use ping to verify when the server is accessible again.

Creating a super-user login on the primary controller

You must add a super-user account, also known as priveledged user account before you use Avaya Installation Wizard to configure the server and install the Avaya authentication file.

Note:

> The passwords you administer for Communication Manager also apply to SES, if SES is optioned.

Note:

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

To create a login:

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

   Note:

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

2. On the Communication Manager System Management Interface main menu, select **Server (Maintenance)** from the **Administration** menu**.**

3. From the navigation menu of the Maintenance Web Pages, select **Security** > **Administrator Accounts**.

   The **Administrator Accounts** screen appears.

4. Select **Add Login**.

5. Select **Privileged Administrator** and click **Submit**.

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

6. Type a login name for the account in the **Login name** field.

7. Verify the following:

   - **susers** appears in the **Primary group** field.
   - **prof18** appears in the **Additional groups (profile)** field. *prof18* is the code for the customer super-user.
   - **/bin/bash** appears in the **Linux shell** field.
   - **/var/home/*login name*** appears in the **Home directory** field, where ***login name*** is the name you entered in step 6.

8. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.

9. For the **Select type of authentication** option, select **password**.

   Note:

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

10. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.

11. In the section **Force password/key change on next login** select **no**.

12. Click **Submit**.

    The system informs you the login is added successfully.

Configuring the S8300

To configure the S8300 server using Configure Server:

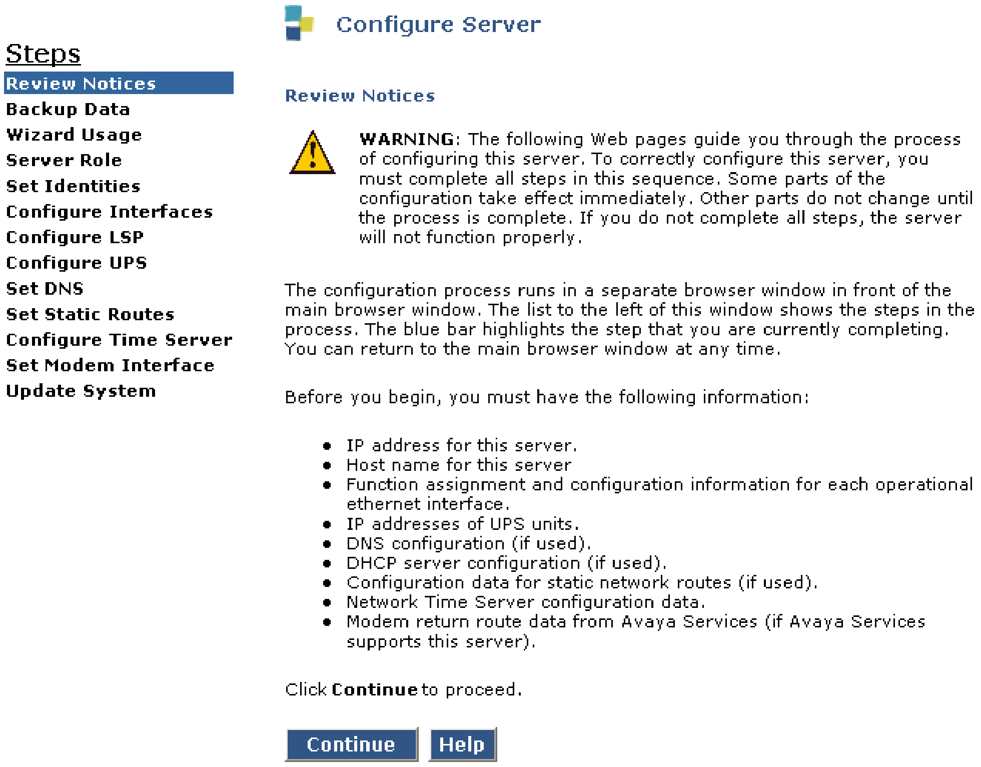
⚠ **CAUTION:**

For a new installation, be sure you have set the time and timezone before proceeding. Failure to do so may cause network problems later.

1. Log in to the Communication Manager System Management Interface.
2. Click **Configure Server** under the **Installation** menu.

   The system displays the **Configure Server** screen.

Configure Server Screen



Review Notices

⚠ **WARNING**: The following Web pages guide you through the process of configuring this server. To correctly configure this server, you must complete all steps in this sequence. Some parts of the configuration take effect immediately. Other parts do not change until the process is complete. If you do not complete all steps, the server will not function properly.

The configuration process runs in a separate browser window in front of the main browser window. The list to the left of this window shows the steps in the process. The blue bar highlights the step that you are currently completing. You can return to the main browser window at any time.

Before you begin, you must have the following information:

- IP address for this server.
- Host name for this server
- Function assignment and configuration information for each operational ethernet interface.
- IP addresses of UPS units.
- DNS configuration (if used).
- DHCP server configuration (if used).
- Configuration data for static network routes (if used).
- Network Time Server configuration data.
- Modem return route data from Avaya Services (if Avaya Services supports this server).

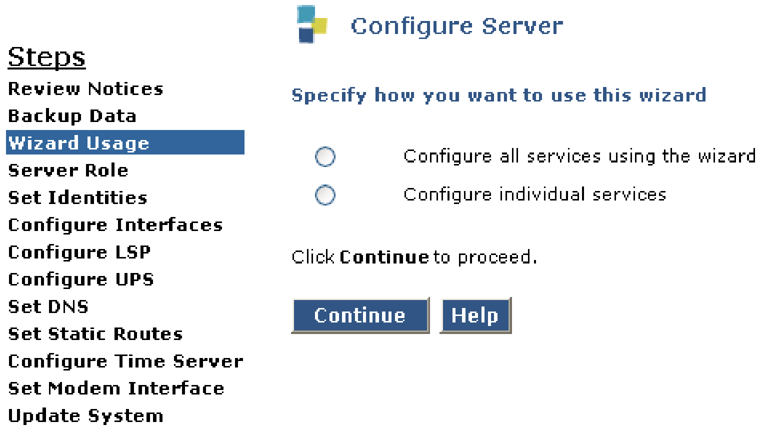
Click **Continue** to proceed.

3. Click **Continue**.

   The system displays the **Back Up Data** Notice screen. Do not perform a backup now.
4. Click **Continue**.

   The **Select Method** screen appears.

Select Method Screen



Configure Server

Specify how you want to use this wizard

○ Configure all services using the wizard

○ Configure individual services

Click **Continue** to proceed.

5. Click **Configure all services using the wizard**.

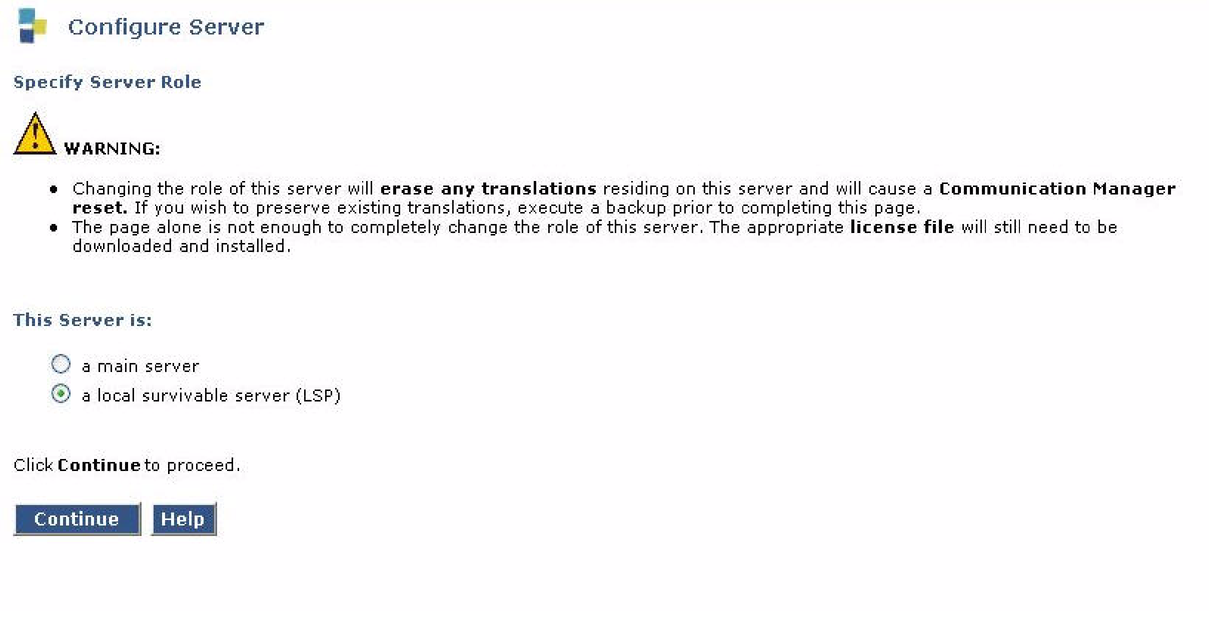
   With this option, the wizard guides you through the screens to configure all of the IP services.

   Note:

   > This option is for the built-in Web Interface configuration wizard, *not* the Avaya Installation Wizard (IW).

6. Click **Continue**.

   The **Specify Server Role** screen appears.



Configure Server

Specify Server Role

WARNING:

- Changing the role of this server will **erase any translations** residing on this server and will cause a **Communication Manager reset.** If you wish to preserve existing translations, execute a backup prior to completing this page.
- The page alone is not enough to completely change the role of this server. The appropriate **license file** will still need to be downloaded and installed.

This Server is:

○ a main server

● a local survivable server (LSP)

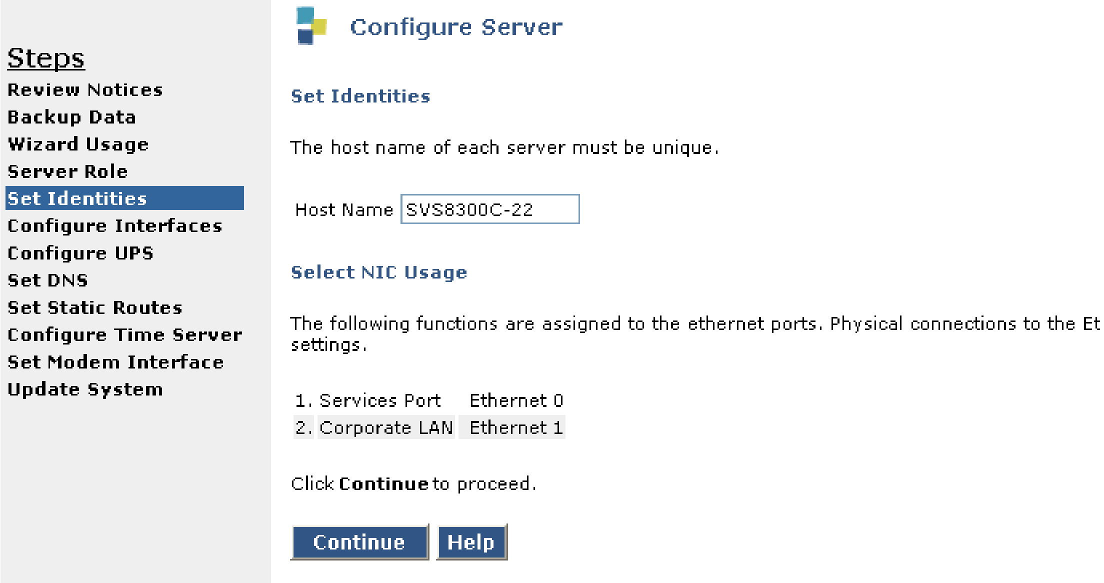
Click **Continue** to proceed.

7. Select the server to be a main server or an LSP server.

8. Click **Continue**.

9. The **Set Identities** screen appears.

Set Identities Screen



Set Identities

The host name of each server must be unique.

Host Name SVS8300C-22

Select NIC Usage

The following functions are assigned to the ethernet ports. Physical connections to the Et settings.

1.	Services Port	Ethernet 0
2.	Corporate LAN	Ethernet 1

Click **Continue** to proceed.

10. Enter the host name for this server in the **Host Name** field (see your planning forms).

The host name uniquely identifies this server.

⚠ **CAUTION:**

If the S8300 on a media gateway is hosting an Communication Manager Messaging application *with Digital Networking*, the name *must* be 10 characters or less.

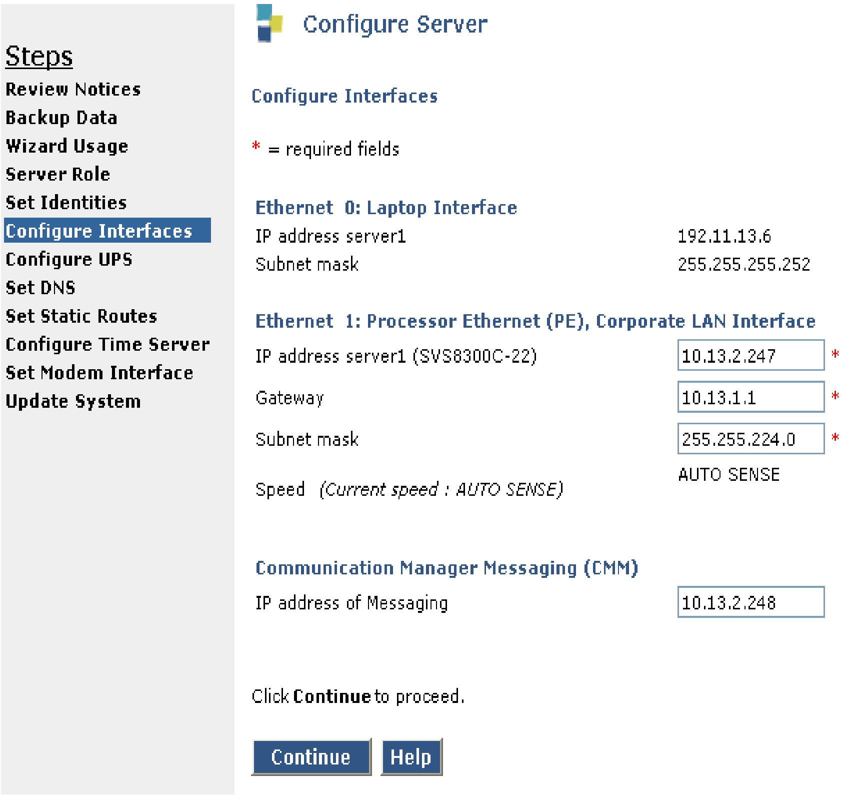
Note:

The screen also lists the current physical cabling to the server. For example, the Services laptop is connected to Ethernet interface 0. Ethernet functions are fixed on the S8300 Server and cannot be changed.

11. Click **Continue**.

The **Configure Interfaces** screen appears.

Configure Interfaces Screen



Configure Server

Configure Interfaces

* = required fields

Ethernet 0: Laptop Interface

IP address server1 192.11.13.6

Subnet mask 255.255.255.252

Ethernet 1: Processor Ethernet (PE), Corporate LAN Interface

IP address server1 (SVS8300C-22) 10.13.2.247 *

Gateway 10.13.1.1 *

Subnet mask 255.255.224.0 *

Speed (*Current speed : AUTO SENSE*) AUTO SENSE

Communication Manager Messaging (CMM)

IP address of Messaging 10.13.2.248

Click **Continue** to proceed.

12. Use your planning forms to complete the fields for the:

- **Ethernet 1: Control Network**
  - **IP Address server1 (*hostname*)** assigned to the S8300 Server.
  - **Gateway** with the IP address of the default gateway of the subnet.
  - **Subnet mask** with the value of the subnet mask of the hosting subnet.
  - **Speed** which should be set to Auto Sense.
- **Communication Manager Messaging (CMM) (if messaging software was installed earlier)**
  - **IP Address of Messagingserver1 (*hostname*)** assigned to Integrated Messaging. Check your planning forms.

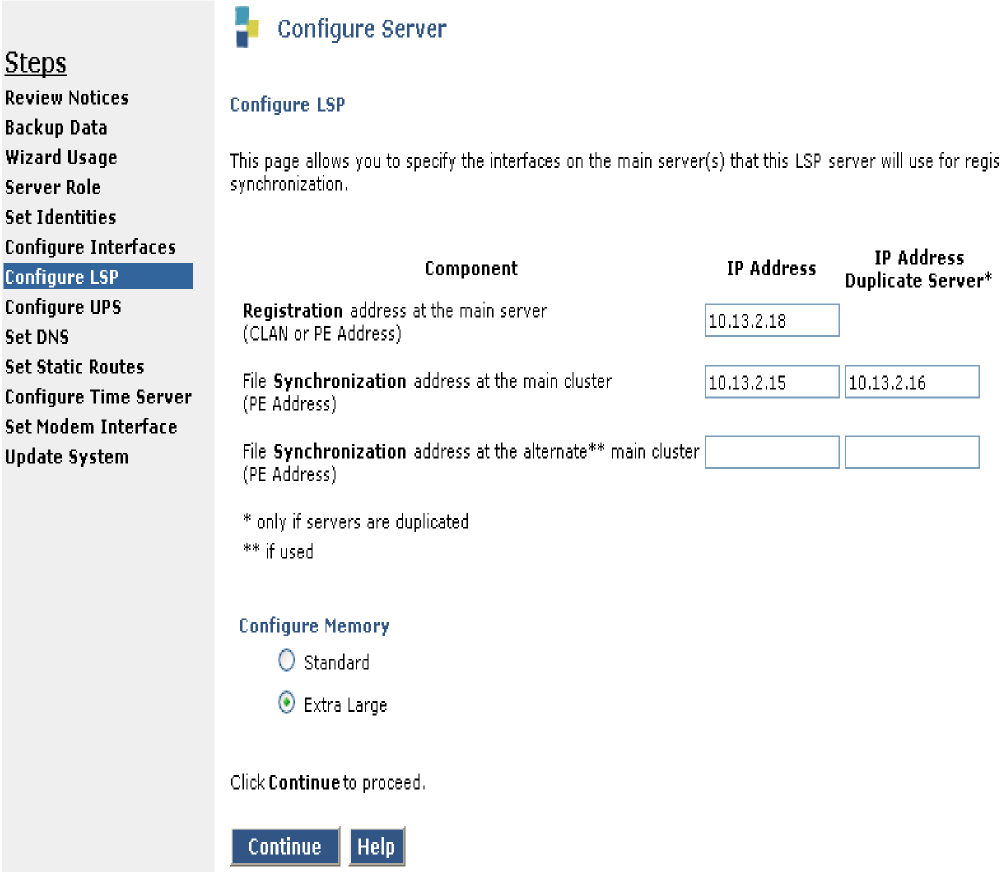
⚠ **CAUTION:**

Do not guess on the addresses on this screen. If you enter the wrong addresses, Integrated Messaging will not be installed, service will be disrupted across the customer's network and may be difficult to correct.

13. Click **Continue**.

The **Configure Local Survivable Processor** screen appears.

Configure Local Survivable Processor Screen



Configure Server

Configure LSP

This page allows you to specify the interfaces on the main server(s) that this LSP server will use for registration and file synchronization.

Component	IP Address	IP Address Duplicate Server*
Registration address at the main server (CLAN or PE Address)	10.13.2.18	
File **Synchronization** address at the main cluster (PE Address)	10.13.2.15	10.13.2.16
File **Synchronization** address at the alternate** main cluster (PE Address)		

* only if servers are duplicated
** if used

Configure Memory

○ Standard

● Extra Large

Click **Continue** to proceed.

14. Configure the LSP server by providing the IP addresses to register the main server, file synchronization address at the main server

    If you clicked the LSP option and the primary controller is an S8300 or S8400 Server, simply enter the IP address of the S8300 server.

    If you clicked the LSP option and the primary controller is an S8500 or S8700-series Server, complete the additional fields as follows:

    - In the **Registration address at the main server** field, enter the IP address of a server's C-LAN or Process Ethernet connected to a LAN to which the LSP or ESS server is also connected. The IP address is used by the LSP or ESS server to register with the main server. In a new installation, where the LSP or the ESS server has not received the initial translation download from the main server, this address will be the only address that the LSP or the ESS server can use to register with the main server.
    - **File synchronization address of the main cluster**: Enter the IP address of a server's NIC connected to a LAN to which the LSP or the ESS server is also connected. The ESS server or the LSP must be able to ping to the address. Consideration should be given to

which interface you want the file sync to use. Avaya recommends the use of the customer LAN for file sync.

Note:

The C-LAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the S8500 or S8700-series. For information on how to upgrade the firmware on the S8500 or S8700-Series, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Servers and Gateways*, 03-300412.

15. Under **Configure Memory**, select **Extra Large** if the S8300 is an LSP supported by an S8720 in an XL configuration or by an S8730. Otherwise, select **Standard**.

    ⚠ **CAUTION:**

    If you select and save as **Extra Large** you cannot revert to **Standard**. If you try to go back to **Standard**, server translation corruption occurs.

16. Click **Continue**.

    The **Configrue UPS** screen appears.

17. In the **Number of UPS Units** field, select the number of Uninterruptible Power Supplies (UPS) units connected to the S8300 Server.

    This number is usually **0** or **1**.

18. If you enter **1** in the **Number of UPS Units** field, enter its IP address in the **UPS 1 IP Address** field.

    The system will use this address to trap power loss signals from the UPS.

19. Click **Continue**.

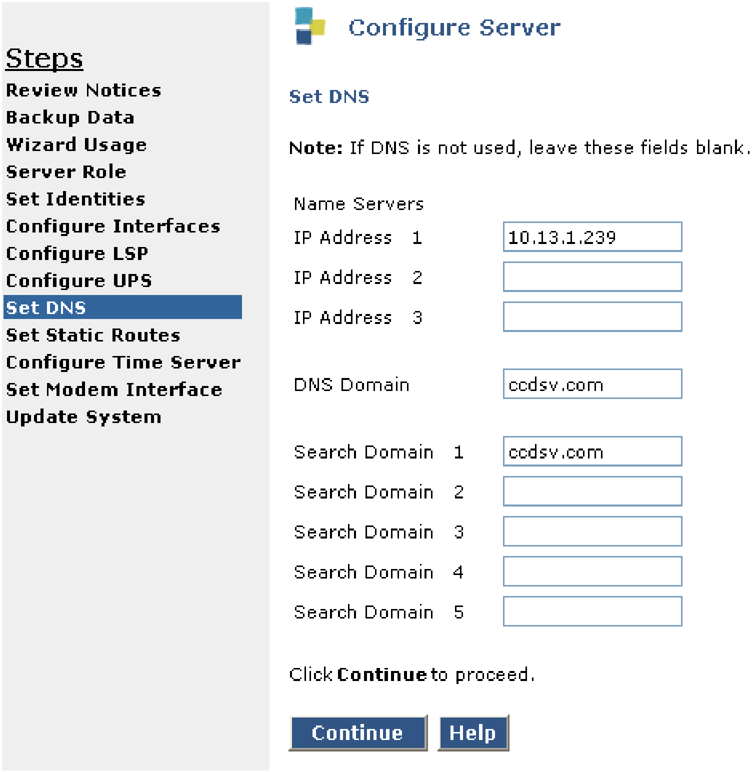
    The **Set DNS** screen appears.

    Most corporate networks have one or more domain name service (DNS) servers that associate an IP address with a device's name. When the DNS is administered with the S8300 Server name, you will be able to access the S8300 server by name as well as IP address over the corporate network.

    ⚠ **CAUTION:**

    (S8300 as a primary controller) If you configure an external DNS server, the DNS will be an extra device that, if not working properly, can cause delays in S8300 access.

Set DNS creen



Set DNS

Note: If DNS is not used, leave these fields blank.

Name Servers	
IP Address 1	10.13.1.239
IP Address 2	
IP Address 3	
DNS Domain	ccdsv.com
Search Domain 1	ccdsv.com
Search Domain 2	
Search Domain 3	
Search Domain 4	
Search Domain 5	

Click **Continue** to proceed.

20. Enter the appropriate IP addresses from your planning documentation.

    Complete the following fields:

    - In the **Name Servers** fields, enter the IP addresses for up to 3 DNS servers on the corporate network.

      The S8300 Server checks the DNS servers in the order in which their addresses are entered for name-to-IP address resolution.

    - In the **DNS Domain** field, enter the name for the part of the network on which the DNS server(s) reside (for example, *mycompany.com*).

      Internet domains are sets of addresses generally organized by location or purpose.

    - In the **Search Domain** fields, **1** to **5**, enter the names of the domains that will be searched, in order, if a user enters an unqualified or incomplete name (such as a host name only without its domain).

    Note:

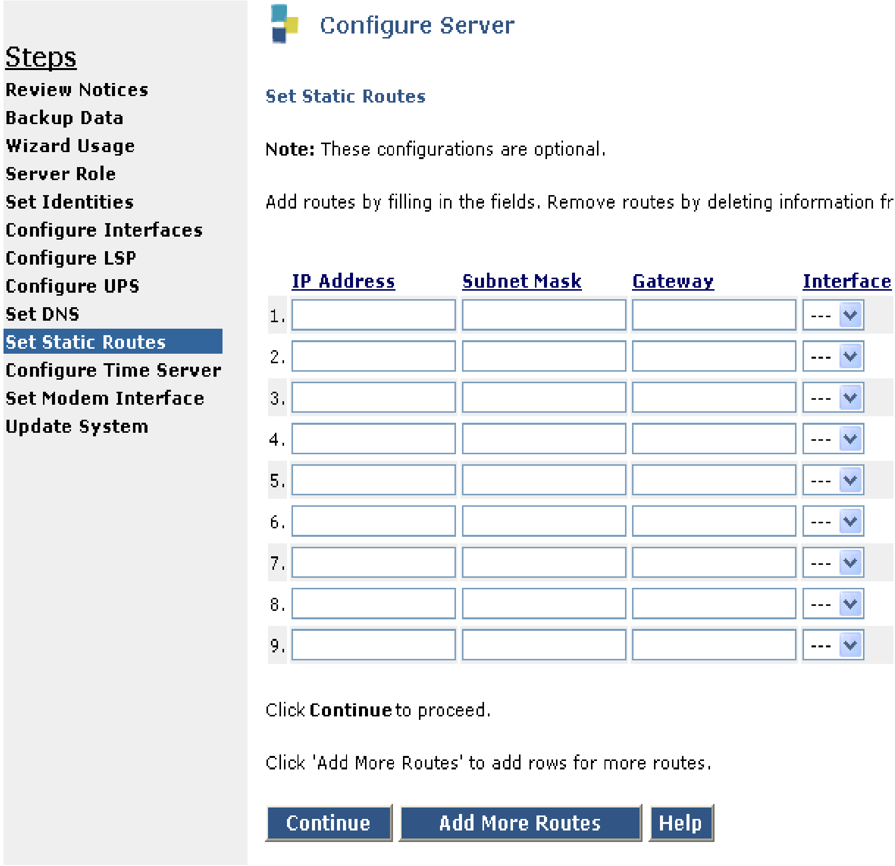
    For **Search Domain 1**, enter the *same domain name* you entered in the **DNS Domain** field above.

21. Click **Continue**.

    The **Set Static Routes** screen appears.

    Static Network Routes are used only if the customer has defined additional routes for IP packets other than through the default gateway. Leave these entries blank, unless the planning documentation supplies routing information.

Set Static Routes Screen



Configure Server

Set Static Routes

Note: These configurations are optional.

Add routes by filling in the fields. Remove routes by deleting information from the fields.

	IP Address	Subnet Mask	Gateway	Interface
1.				---
2.				---
3.				---
4.				---
5.				---
6.				---
7.				---
8.				---
9.				---

Click **Continue** to proceed.

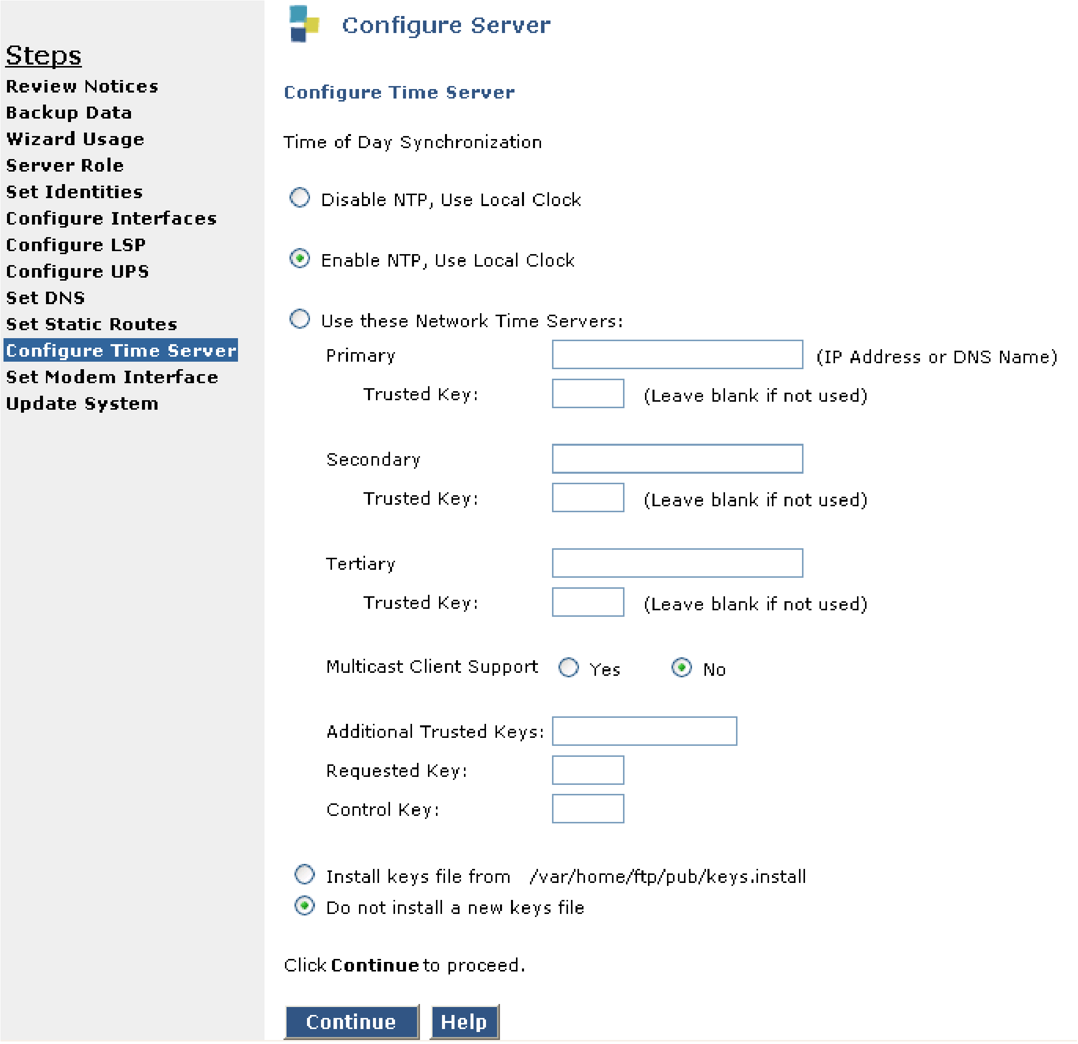
Click 'Add More Routes' to add rows for more routes.

22. Click **Continue**.

    The system displays the **Configure Time Server** screen.

    The **Configure Time Server** screen allows you to set up the Network Time Protocol (NTP) Service.

Configure Time Server Screen



Configure Server

Configure Time Server

Time of Day Synchronization

○ Disable NTP, Use Local Clock

● Enable NTP, Use Local Clock

○ Use these Network Time Servers:

Primary		(IP Address or DNS Name)
Trusted Key:		(Leave blank if not used)
Secondary		
Trusted Key:		(Leave blank if not used)
Tertiary		
Trusted Key:		(Leave blank if not used)

Multicast Client Support ○ Yes ● No

Additional Trusted Keys:

Requested Key:

Control Key:

○ Install keys file from /var/home/ftp/pub/keys.install

● Do not install a new keys file

Click **Continue** to proceed.

Make the following choices, according to the planning documentation:

- Choose **Disable NTP** if the user does not want the Network Time Protocol to run on the S8300 Server.

  Select this option to disable Network Time Protocol (NTP) and use the S8300 Server's own clock as a time source. You typically choose this option if this is the only S8300 Server in the configuration and it will not be synchronized with an external time source.

- Choose **Enable NTP** if the S8300 Server will be the primary NTP server.

  Optionally, you can provide the address of the survivable S8300 Server in the local survivable configuration. Select this option to enable NTP and use the S8300 Server's own clock as a time source. You typically choose this option if there is more than one S8300 Server in the configuration (for example, this or another S8300 Server may be acting as an LSP standby unit), and an external time source is not available to provide synchronization between the units. Select this option to enable NTP and use its own clock as a time source. You need to set up the time clock with Set Server Time/Timezone option. You need to set the server clock using the Set Server Time / Timezone screen. You can do this now, then return to the Configure Server window.

- Choose **Use these Network Time Servers** to enter up to three time servers.

  Select this option to enable NTP and be synchronized with an external time source on the corporate network.

23. If you did not select **Use these Network Time Servers** in the previous step, click **Continue** and go to the next step.

    If you selected **Use these Network Time Servers** in the previous step, complete the following fields:

    Specify up to three network time servers by IP address or DNS name in the order in which you want the S8300 Server to check them. You should always specify at least two.

    - **Primary** — Enter an IP address or DNS name.

      If a trusted key is required, enter a valid key number in the **Trusted Key** field.

    - **Secondary** — Enter an IP address or DNS name.

      If a trusted key is required, enter a valid key number in the **Trusted Key** field.

    - **Tertiary** — Enter an IP address or DNS name.

      If a trusted key is required, enter a valid key number in the **Trusted Key** field.

    - **Multicast Client Support** — Select **Yes** if the NTS routinely broadcasts its timing messages to multiple clients.

      Select **No** if the S8300 Server is to poll (directly request the time from) the NTS.

    - **Additional trusted keys** (optional) — If you want to encrypt the messages between an NTS and the S8300 Server, list the valid key numbers, up to 3, provided by your LAN administrator on the pre-installation worksheet.

      Trusted keys function like a checksum to make sure the time packets are valid. Use a blank space as a delimiter if there is more than one key (for example, 2 3 6 to specify valid keys 2, 3, and 6). These numbers are associated with encryption codes in a "keys" file.

    - **Request key** — Enter a key to send a remote query request.

      Only 1 key is allowed in this field.

    - **Control key** — Enter a key to query and request changes to an NTS.

      Only 1 key is allowed in this field.

24. If you have a file named *keys.install* to allow the S8300 Server to communicate with the NTS, select **Install keys from var/home/ftp/keys.install**.

    If you do not have a keys.install file, select **Do not install a new keys file**.

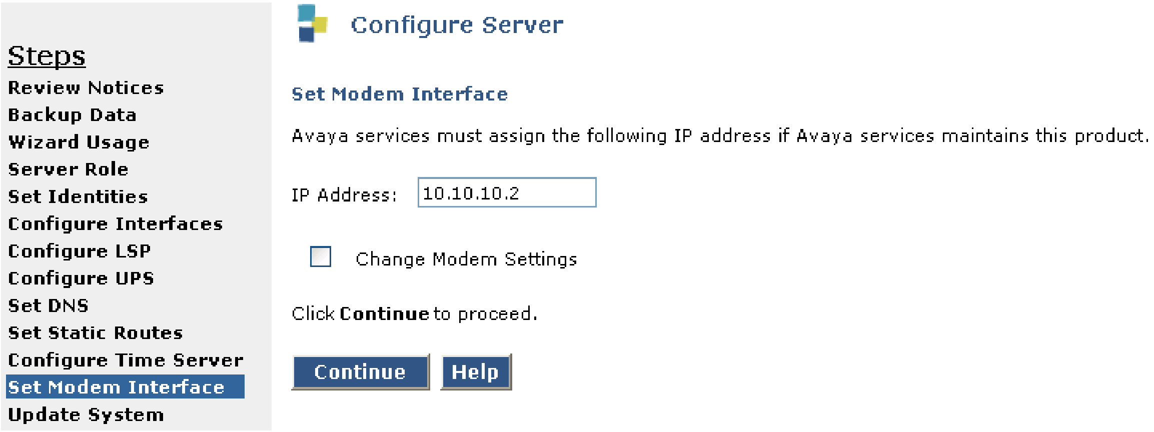
    Note:

    > If you have a *keys.install file*, upload or create it now, if possible. See Providing the keys.install file (If necessary) on page 238. If you upload the keys file later, you have to run the Web Interface Configure Server wizard again to have the system recognize it.

    Click **Continue**.

25. At the next screen, **Set Modem Interface**, you can set up the Modem Interface IP Address for Avaya-provided service.

Set Modem Interface Screen



Set Modem Interface

Avaya services must assign the following IP address if Avaya services maintains this product.

IP Address: 10.10.10.2

□ Change Modem Settings

Click **Continue** to proceed.

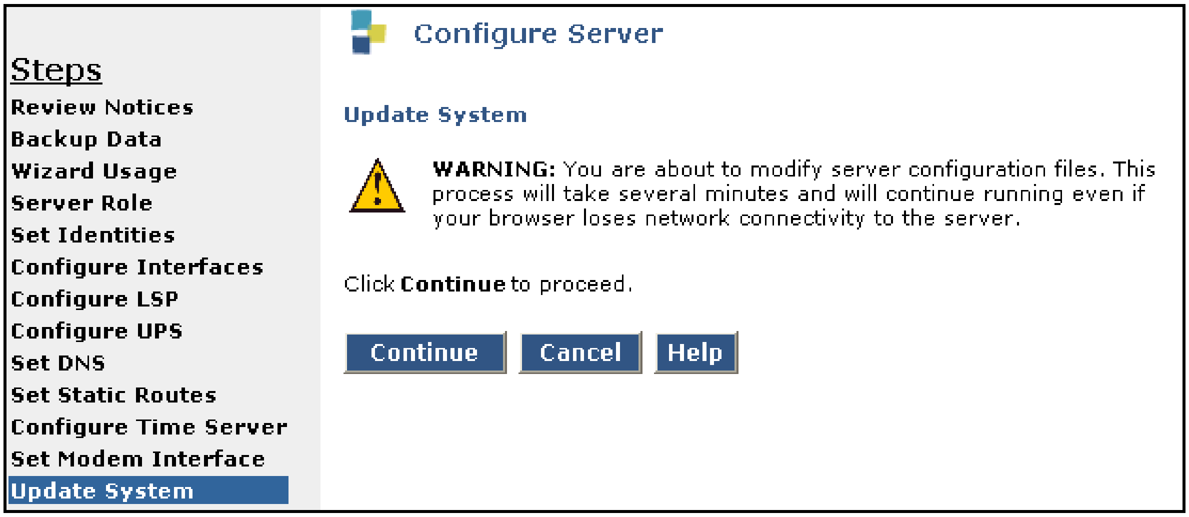
Note:

> The Modem IP Address for the Avaya INADS alarming is assigned by the ART tool. You should have obtained this address when you performed Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary on page 216.

26. Click **Continue**.

    The next **Warning** screen indicates that the data entry process has concluded and that the system is ready to be configured.

Warning Screen



Configure Server

Update System

WARNING: You are about to modify server configuration files. This process will take several minutes and will continue running even if your browser loses network connectivity to the server.

Click **Continue** to proceed.

Note:

> This is the final step in configuring the system. When you click **Continue**, all the configuration information will be written to disk and implemented. This step normally completes in about 5 minutes.
>
> This is your last chance to cancel or correct the configuration.

27. To check, or possibly change, something you entered on a previous screen, use your browser's **Back** button to page back through the **Configure Server** screens.
28. Check or change the items in question.
29. Click the **Continue** button to move forward again, whether you change anything or not.

    If you don't do this, information in the wizard may not be processed correctly.

    Note:

    > For any configuration, it is always safe to **Cancel** the configuration, and run the Configure Server screens of the Web Interface again later from the beginning. You might use this option if you are checking or modifying settings on a server that has already been configured, and there is not a large amount of new information to enter.

30. On the **Update System** screen, if you are satisfied that everything is set correctly, click **Continue**.

    You can watch the progress of the configuration at the **Updating System Files** screen. If the configuration status displays stops updating at some point and the screen appears to freeze, you may have lost contact with the server. In this case, the configuration process will continue and you can log back on and pick up where left off.

    When the process is complete, you will receive a notification.

31. Click **Close Window** and continue the configuration of the media gateway on the command line interface.

Providing the keys.install file (If necessary)

Use this procedure only if you selected one of the customer-provided keys options in the previous procedure.

If encryption between the NTS and S8300 Server is to be used for additional security, you *must* provide a keys.install file that specifies for each key:

- The key number
- The encryption type
- The key code

If the keys file is short, the network administrator can create one now during configuration if needed.

To create the key file

1. On a directly connected laptop or other computer, create a flat-text file named *keys.install*, with the correct keys information using any ASCII application (for example, Notepad).
2. Upload the *keys.install* file using the **Upload Files to Server** screen as described earlier.
3. When finished, click the **Configure Server** wizard window to resume server configuration.

The keys file can be loaded in one of the following two ways. If a *keys.install* file was previously created on or downloaded to the services laptop or another computer on the network, it can be installed now, as follows:

To upload the keys file

1. In the main menu under **Miscellaneous**, click the **Upload Files to Server** link.
2. Locate the *keys.install* file on your computer or network, then click **Load File**.

   The file is uploaded to the S8300 Server's FTP directory.
3. When finished, click the **Configure Server** wizard window to resume server configuration.

Longer files may be transferred from the network time server to the S8300 Server as follows:

To download or copy the keys file

1. Using either the **Download Files to Server** screen or the Transfer files using an FTP procedure to access the keys file listed on your pre installation worksheet.

   In both cases, the file is transferred to the S8300 Server's FTP directory.
2. When finished, click the **Configure Server** wizard window to resume server configuration.
3. After the keys.install file is uploaded, select the location where it resides, usually in the **/var/home/ftp** subdirectory. (Services personnel may direct you to use the /tmp directory.)
4. If a keys file is not used, or if the correct *keys.install* file is already installed, select the option not to install a new keys file.

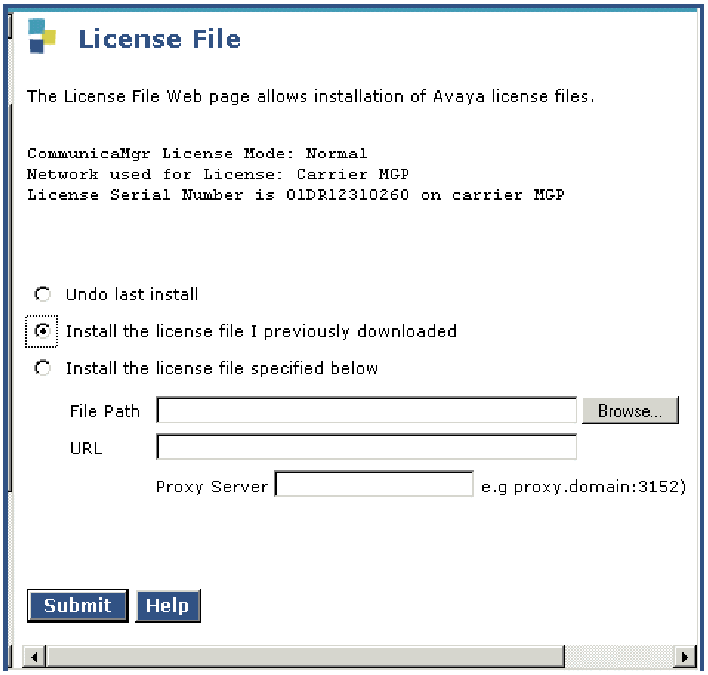
Installing the Communication Manager license

To install the license and authentication files

1. Under Security, select **License File**.

   The **License File** screen appears.

License File Screen



The License File Web page allows installation of Avaya license files.

```
CommunicaMgr License Mode: Normal
Network used for License: Carrier MGP
License Serial Number is 01DR12310260 on carrier MGP
```

○ Undo last install

● Install the license file I previously downloaded

○ Install the license file specified below

File Path

URL

Proxy Server e.g proxy.domain:3152)

2. Select **Install the license file I previously downloaded** and click **Submit**.

   The system displays the **License File Install Results** screen.

3. Click the **Restart CM** button, if it is displayed on the screen.

Installing the Communication Manager authentication files

Note:

Skip this task if you are installing the S8300 as an LSP.

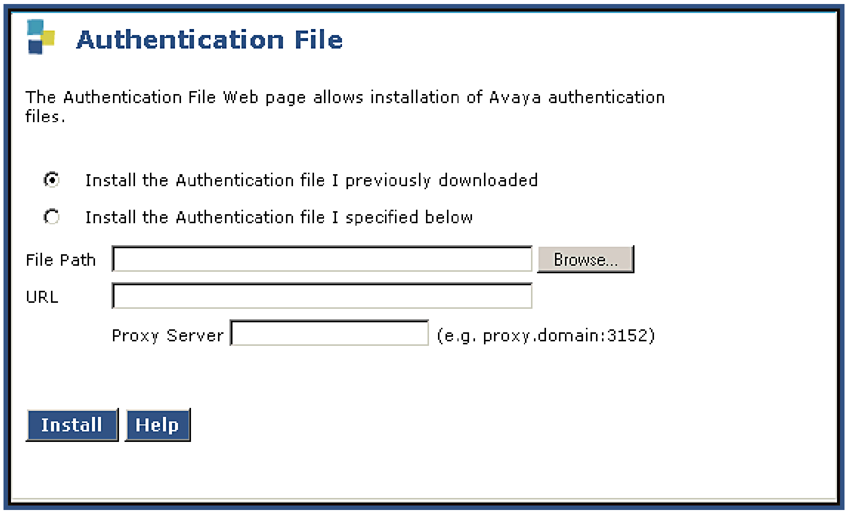
⚠ **CAUTION:**

A super-user login, dadmin, or other customer super-user login must exist *before* you install an authentication file. See Creating a super-user login on the primary controller on page 224.

1. Under Security, select **Authentication File**.

   The **Authentication File** screen appears.

Install Authentication Screen



Authentication File

The Authentication File Web page allows installation of Avaya authentication files.

● Install the Authentication file I previously downloaded

○ Install the Authentication file I specified below

File Path

URL

Proxy Server (e.g. proxy.domain:3152)

2. Select **Install the license file I previously downloaded** and click **Submit**.

   The system displays the License File Install Results screen.

3. Click the **Restart CM** button, if it is displayed on the screen.

4. Verify the license and authentication file installation by issuing the `statuslicense -v` command from the server command line:

   - The **License Mode** should be **Normal**.
   - The report should list a **License Serial Number**.

If the server is an LSP, stop and start Communication Manager

Note:

> Skip this task if you used the Restart CM button just after loading the license file for this LSP. See, Installing the Communication Manager authentication files on page 240.

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

2. Type `stop -caf`.

3. Type `start -ca`.

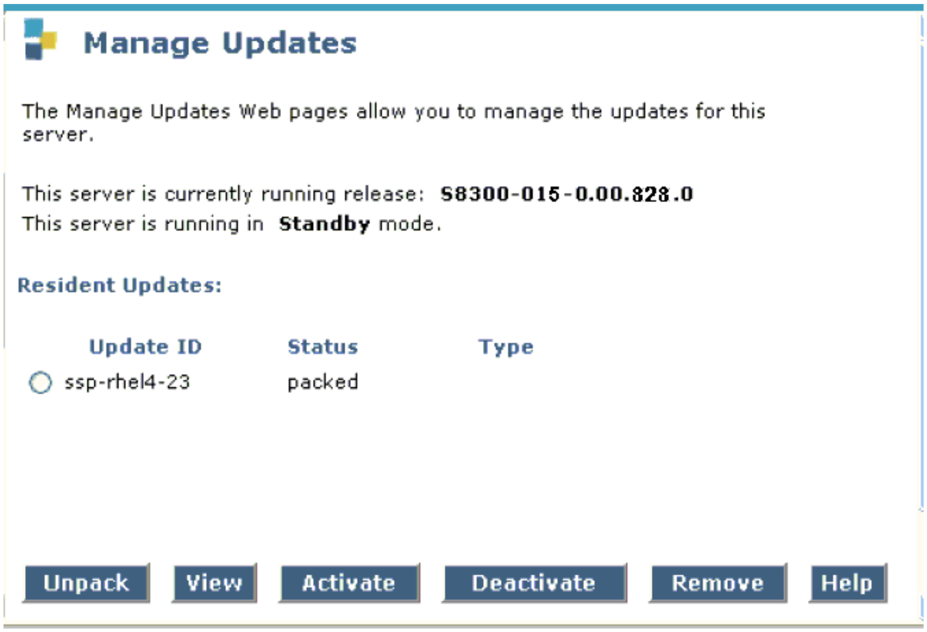
Installing security files, Communication Manager service packs and SES service packs, if any

To install security files and/or service packs

1. Under Server Upgrades, select **Manage Updates**.

   The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allow you to manage the updates for this server.

This server is currently running release: **S8300-015-0.00.828.0**
This server is running in **Standby** mode.

Resident Updates:

	Update ID	Status	Type
○	ssp-rhel4-23	packed	

2. Do one or both of the following:

   a. If there are earlier versions of files that you are updating, select those versions and click **Deactivate**.

      The screen shows the status of the deactivation.

   b. If a file you want to activate shows **packed** in the **Status** column, select that file and click **Unpack**.

      The screen shows the status of the unpacking.

3. Check the **Type** column for the file you want to activate. Tell the customer that the system will reboot if the file type is **cold**. The customer may want to wait to install this security update.

4. Select the file you want to activate and click **Activate**.

   The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

Saving translations

Note:

If the S8300 you are installing is an ***LSP***, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session and log in as *craft* (or *dadmin*).
2. If the S8300 you are installing is a primary controller, at the SAT prompt, type **`save translation`** and press **Enter**.
3. If the S8300 you are installing is an LSP, then on the primary controller, type **`save translation lsp`** and press **Enter**. This command distributes saved translations out to the LSPs.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

   The LSP automatically performs a reset system.

Enabling SIP Enablement Services, if desired

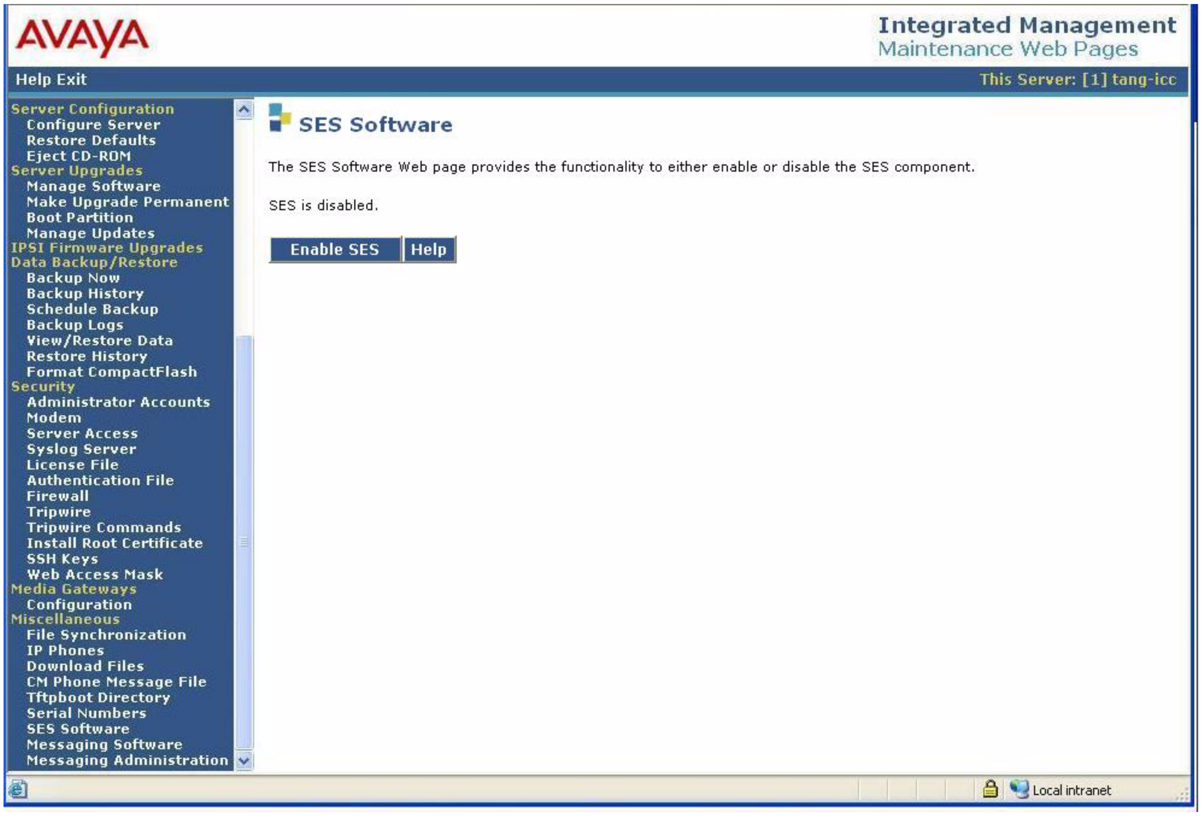
If the S8300, as a primary controller only, is going to run SIP Enablement Services (SES) software, perform this task

To enable SES

1. On the **Server (Maintenance)** Web page, select **Miscellaneous > SES Software**.

   The **SES Software** screen appears, and the text, "SES is disabled" appears just above the **Enable SES** button.

SES Software screen



The SES Software Web page provides the functionality to either enable or disable the SES component.

SES is disabled.

2. Click **Enable SES**.
3. Wait approximately 30 seconds and click the refresh button on your browser.

   The **SES Software** page should show, "SES is enabled."

To verify SES is enabled

1. Return to the S8300 Web interface Welcome page, and refresh your browser.
2. On the main menu for the Communication Manager System Management Interface, verify that the **SIP Enablement Services** option is now available under **Administration** menu.

   Note:

   You must also install the SES license and administer SES. See Installing the SES license on page 269 and SES administration tasks on page 271.

Configuring and Installing firmware on a Media Gateway

You need to configure the media gateway in which the S8300 Server is mounted. For example, if media gateway is a G450, you need to:

- Define a new interface and its IP address
- Configure parameters that identify the G450 to other devices
- Define a G450 interface as the G450's default gateway
- Configure an MGC to work with the G450
- Configure DNS resolver for resolving hostnames to IP addresses
- View the status of the G450
- Manage and upgrade software, firmware, configuration, and other files on the G450
- Backup and restore the G450

For more information on configuring the G450 gateway, refer "Chapter 5, Basic Device Configuration" of the *Administration for the Avaya G450 Media Gateway*, 03-602055 guide.

For more information on upgrading the firmware on the G450 gateway, refer "Chapter 10, Upgrading the G450 firmware" of the *Installing and Upgrading the Avaya G450 Media Gateway*, 03-602054 guide.

Similarly, refer the appropriate documentation if the a different gateway is used with the S8300 Server.

Administering Communication Manager

⚠ **Important:**

The administration procedures in this section are performed on the primary controller.

If the S8300 just installed is a primary controller, administer the S8300 primary controller using Adminstering an S8300 primary controller on page 259. This configuration of Media Gateway and S8300 Server is known as Internal Call Controller (ICC).

If the S8300 just installed is an LSP, and the primary controller of this S8300 LSP is an S8300 server, administer the primary controller using Administering an S8300 primary controller on page 246. This configuration of Media Gateway and S8300 LSP Server is known as External Call Controller (ECC).

If the S8300 just installed is an LSP, and the primary controller of this S8300 LSP is an S8400, S8500/S8510, or S8700-series server, administer the primary controller using Administering an S8400, S8500, or S8700-Series primary controller when the S8300 is an LSP on page 253.

This configuration of Media Gateway and S8300 LSP Server is known as External Call Controller (ECC).

Perform one of the following two administration procedures in this section:

- Administering an S8300 primary controller
- Administering an S8400, S8500, or S8700-Series primary controller when the S8300 is an LSP

Administering an S8300 primary controller

⚠ **CAUTION:**

> This administration applies only to the primary controller. If the S8300 you installed is configured as an LSP, do *not* perform this administration on it. Translations are automatically copied to the LSP from the S8300 primary controller.

Skip this section and go to Administering an S8400, S8500, or S8700-Series primary controller when the S8300 is an LSP on page 253 if the primary controller is an S8400, S8500, or S8700-series Server.

This document covers only the administration of Communication Manager required for a media gateway to communicate with the primary controller over a customer's network. For the majority of administration required, see *Administering Avaya Aura™ Communication Manager*, 03-300509, or *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

In this section, you will use the SAT interface to:

- Assigning Node Names and IP Addresses for the LSPs
- Administering Network Regions
- Associating LSPs with Network Regions
- Administering the IP address map
- Administering IP Interfaces
- Identifying LSPs to the S8300 primary controller
- Saving translations

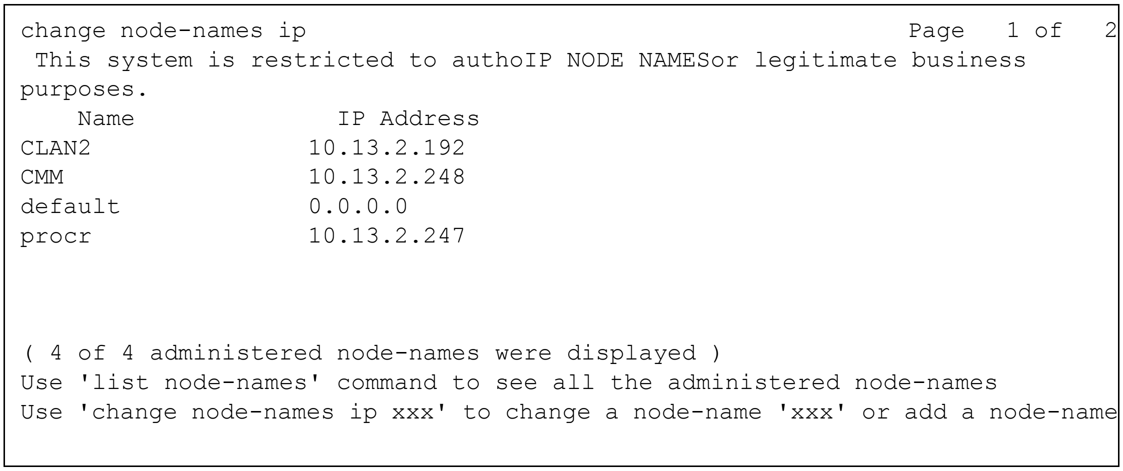
Assigning Node Names and IP Addresses for the LSPs

If the S8300 network configuration includes LSPs, they must be specified on the **Node Names** screen.

To assign node names

1. At the S8300 SAT prompt, type **`change node-names ip`** to open the **Node Names** screen.

Example Node Names Screen



```
change node-names ip                                          Page   1 of   2
 This system is restricted to authoIP NODE NAMESor legitimate business
purposes.
    Name                  IP Address
CLAN2                   10.13.2.192
CMM                     10.13.2.248
default                 0.0.0.0
procr                   10.13.2.247



( 4 of 4 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

2. Enter the name and IP addresses for the LSPs.
3. Press **F3** (**Enter**) when complete.

Administering Network Regions

Before assigning an IP network region to a media gateway, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a media gateway with an S8300 as primary controller, there could be one network region, defined as **1**. The procedure below uses 1 for the network region number as an example but the procedure applies for any network region number from 1 to 250.

To define IP network region 1

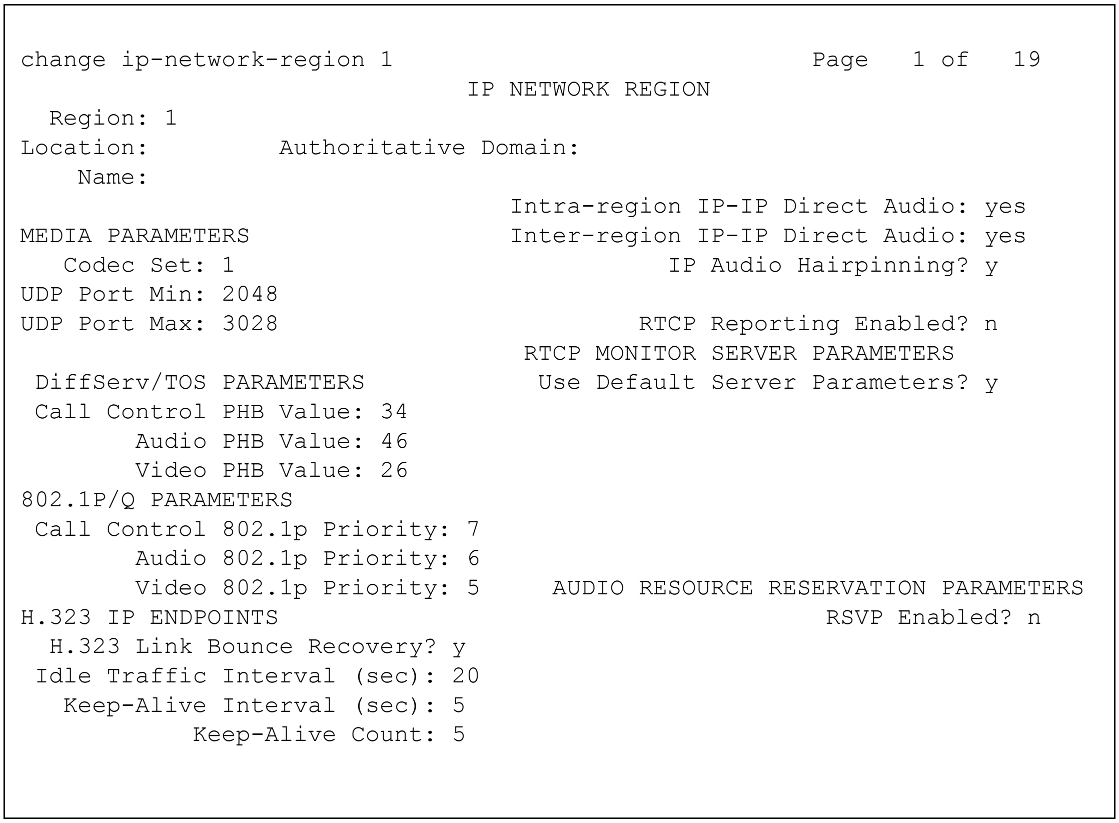
CAUTION:

Defining IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

1. At the SAT prompt, type **`change ip-network-region 1`**.

   The S8300 displays the **IP Network Region** screen.

IP Network Region Screen



```
change ip-network-region 1                             Page   1 of   19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
                                  Intra-region IP-IP Direct Audio: yes
MEDIA PARAMETERS                  Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                              IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028                         RTCP Reporting Enabled? n
                                   RTCP MONITOR SERVER PARAMETERS
 DiffServ/TOS PARAMETERS            Use Default Server Parameters? y
 Call Control PHB Value: 34
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

2. If necessary, complete the fields as described in *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. Press **F3** (**Enter**) to submit the screen.

Associating LSPs with Network Regions

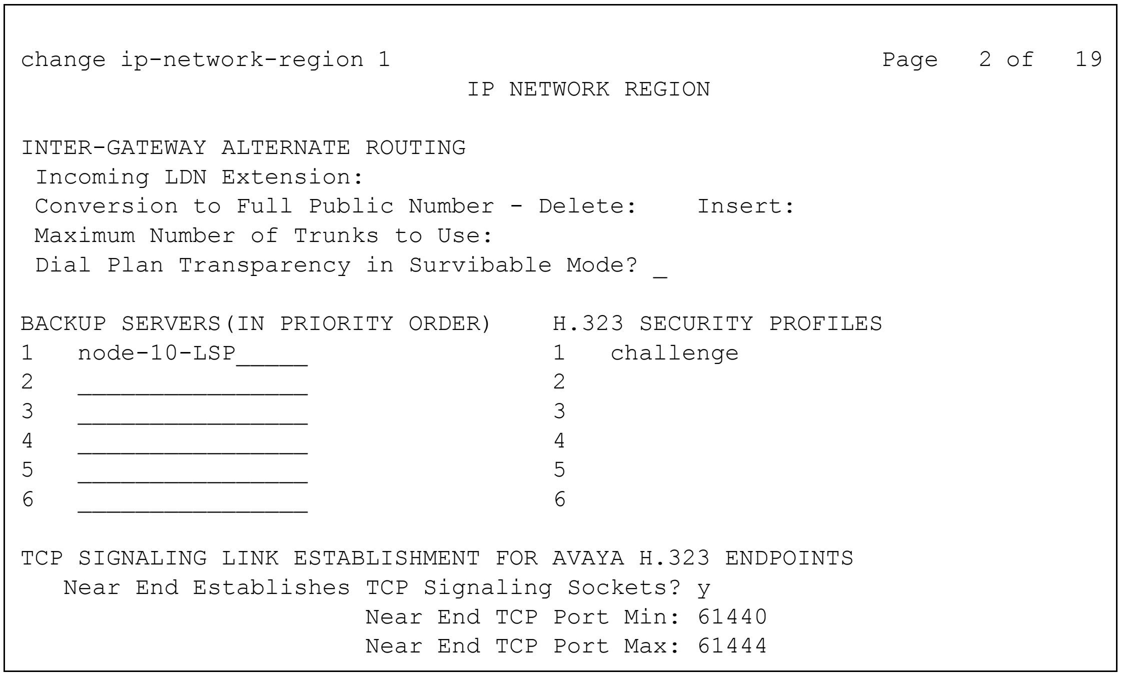
If the primary controller has LSPs, you can associate each LSP with one or more network regions. In the event of a network failure, IP telephones assigned to a network region will register with an LSP associated with that region.

This procedure associates up to six LSPs with a network region.

To associate LSPs with a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2



```
change ip-network-region 1                                  Page   2 of   19
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING
 Incoming LDN Extension:
 Conversion to Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use:
 Dial Plan Transparency in Survibable Mode? _

BACKUP SERVERS(IN PRIORITY ORDER)     H.323 SECURITY PROFILES
1   node-10-LSP_____                  1   challenge
2   ________________                  2
3   ________________                  3
4   ________________                  4
5   ________________                  5
6   ________________                  6

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Sockets? y
                        Near End TCP Port Min: 61440
                        Near End TCP Port Max: 61444
```

2. Enter the names of up to six LSPs to be associated with region 1.

   The LSP names must be the same as administered on the **Node Names** screen.

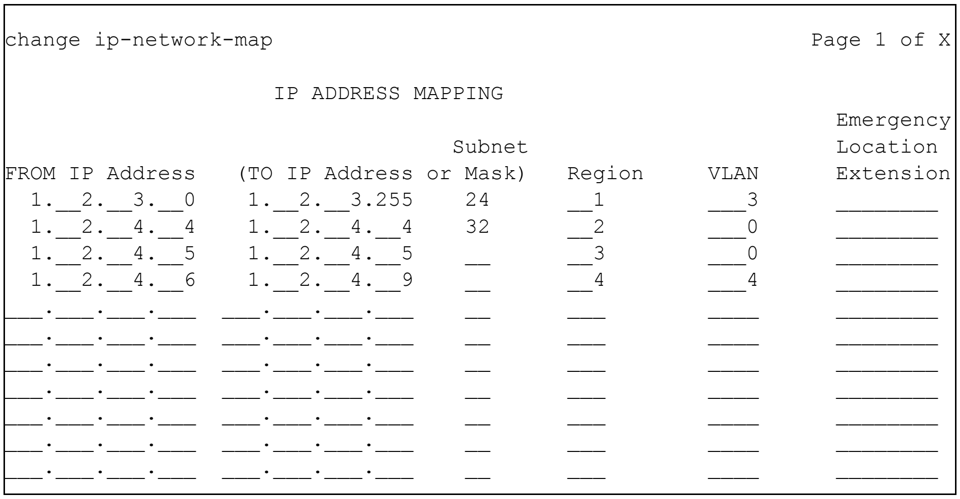
3. Submit the form.

4. Repeat for each network region with which you want to associate LSPs.

Administering the IP address map

Administer the IP address map to assign IP phones and other IP endpoints to the same network region as the media gateway.

1. Type **`change ip-network-map`** and press **Enter** to display the IP Address Mapping screen.



```
change ip-network-map                                           Page 1 of X

                     IP ADDRESS MAPPING
                                                                  Emergency
                                   Subnet                         Location
FROM IP Address   (TO IP Address or Mask)   Region     VLAN       Extension
  1.__2.__3.__0    1.__2.__3.255    24       __1       ___3       ________
  1.__2.__4.__4    1.__2.__4.__4    32       __2       ___0       ________
  1.__2.__4.__5    1.__2.__4.__5    __       __3       ___0       ________
  1.__2.__4.__6    1.__2.__4.__9    __       __4       ___4       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
___.___.___.___  ___.___.___.___    __       ___       ____       ________
```

2. In the **FROM IP Address** and **TO IP Address** fields, enter a range of IP addresses for IP phones or other IP endpoints connected to the media gateway.
3. In the **Region** field, enter the network region to which the media gateway and its IP endpoints are to be assigned.
4. In the **VLAN** field, enter the VLAN number the IP endpoints should be a member of. Each network region should have its own VLAN number.
5. Enter an extension number in **Emergency Location Extension** field.

   Note:

   For more detail about the IP Address Mapping form, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Administering IP Interfaces

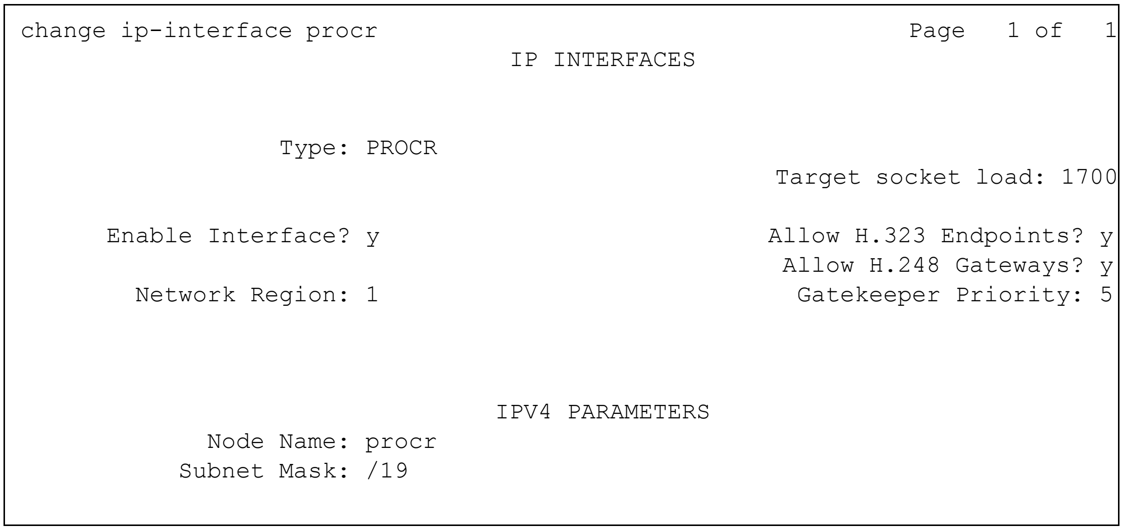
This procedure assigns network region 1, as an example, to the S8300 Server.

To assign the network region and IP endpoint access to the S8300

1. At the SAT prompt, type **`change ip-interfaces procr`**.

   The S8300 displays the **IP Interfaces** screen for the S8300 Server.

IP Interfaces Screen



```
change ip-interface procr                                    Page   1 of   1
                                  IP INTERFACES


                  Type: PROCR
                                                          Target socket load: 1700

      Enable Interface? y                                Allow H.323 Endpoints? y
                                                          Allow H.248 Gateways? y
        Network Region: 1                                  Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /19
```

2. The field **Enable Ethernet?** should indicate `y` (yes)**.** The **Node Name** should be the IP address of the S8300 Server.
3. In the **Allow H.323 Endpoints** field, enter a ’y’ to allow H.323 endpoint connectivity to the server.
4. In the **Allow H.248 Endpoints** field, enter a ’y’ to allow H.248 media gateway connectivity to the server.
5. In the **Gatekeeper Priority** field, enter a value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to **y**.
6. In the **Target Socket Load** field, enter the maximum number of sockets targeted for this interface. The default is 80% of the maximum of 2000. When all the IP interfaces within the same Gatekeeper Priority exceeds the target number that you allocate, the system continues to add sockets until the interface is at its maximum capacity.

Identifying LSPs to the S8300 primary controller

If the primary controller has LSPs, you must enter the LSP node names on the Survivable Processor form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the survivable-processor screen, their status can be viewed with the **`list survivable-processor`** command.

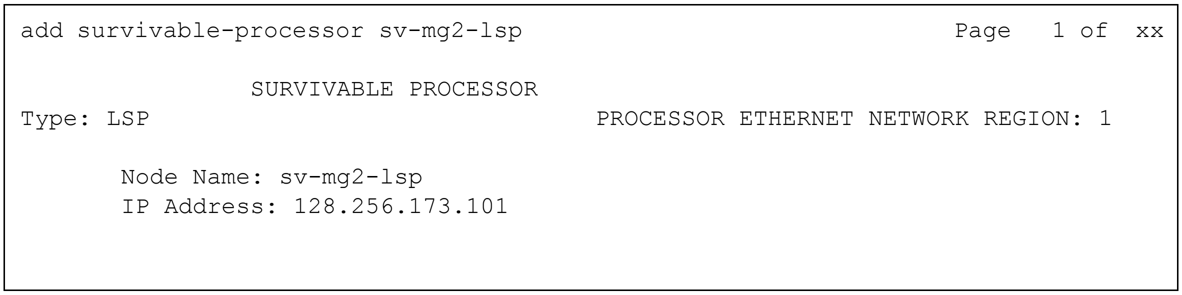
Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **Survivable Processor** screen.

1. At the SAT command line, type **`add survivable-processor`** ***<name>,*** where ***<name>*** is the LSP name from the Node Names screen.

   The Survivable Processor screen appears.

Figure 16: Add Local Survivable Processor screen



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

                SURVIVABLE PROCESSOR
Type: LSP                                PROCESSOR ETHERNET NETWORK REGION: 1

       Node Name: sv-mg2-lsp
       IP Address: 128.256.173.101
```

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Node Name is a display-only field that shows the name used to identify this server. You enter node names through the IP Node Names screen.
4. IP Address is a display-only field that shows the IP address that corresponds to the node name you entered.
5. Enter a Processor Ethernet Network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support. Valid values can be from 1 to250. Enter the network region in which the PE interface of the LSP resides.

   Note:

   With the LSP now administered on the primary controller, the LSP can register.
6. At the SAT, type list survivable-processor to verify that the LSP is registered.

Skip to Administering the Media Gateway on page 264.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **`save translation lsp`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

   Note:

   If the LSP is registered to the primary controller, the **`save translation lsp`** command transfers the super-user and other accounts from the primary controller to the LSP.

Administering an S8400, S8500, or S8700-Series primary controller when the S8300 is an LSP

In this case, the S8300 you have installed is configured as an LSP.

⚠ **CAUTION:**

This administration applies only to the primary controller that controls the S8300 LSP that you are installing. The primary controller can be an S8400, S8500, or S8700-series Server. Do *not* administer the S8300 LSP. Translations are automatically copied to the LSP from the primary controller.

Skip this section and go to Administering an S8300 primary controller on page 246 if the primary controller is an S8300.

Note:

Some of the procedures in this section may have been completed previously as part of a normal S8300 Server installation.

For the majority of required administration, see *Administering Avaya Aura™ Communication Manager*, 03-300509, or *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

In this section, you will use the SAT interface on the primary controller to:

- Assigning Node Names and IP Addresses for the C-LANs and LSPs
- Administering Network Regions
- Administering the IP address map
- Administering IP Interfaces
- Identifying the Survivable Processor on the primary controller
- Saving translations

Note:

For information on installing the CLAN boards on the S8400, S8500, or S8700-series port networks and complete information on installing an S8400, S8500, or S8700-series Server, see the Installation documentation on the *Documentation for Avaya Aura™ Communication Manager, Media Gateways and Servers CD*, 03-300151.

Assigning Node Names and IP Addresses for the C-LANs and LSPs

Note:

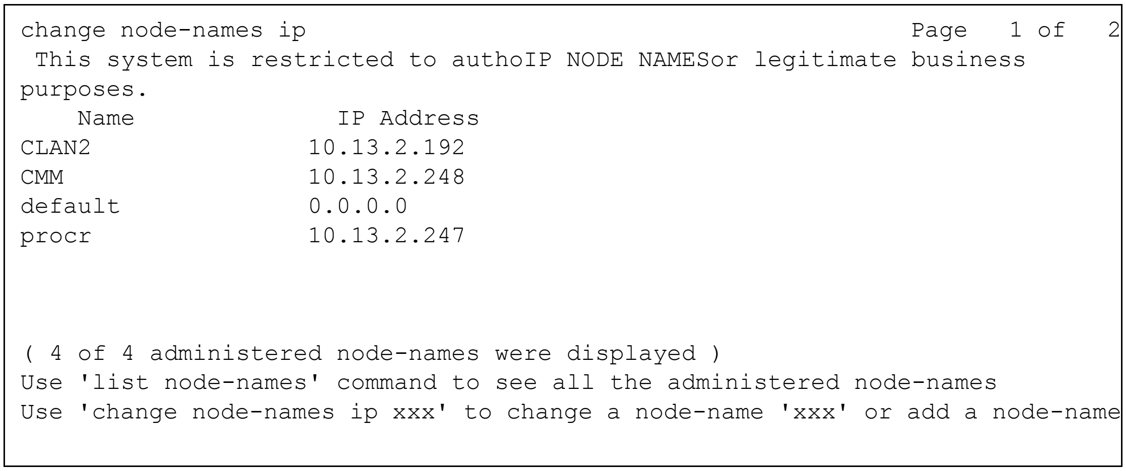
The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the S8300 Server. For information on how to upgrade the firmware on the S8400, S8500 or S8700-series Server, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Servers and Gateways*, 03-300412.

To assign node names and IP addresses

Note:

At the SAT prompt, type **`change node-names ip`** to open the **Node Names** screen.

Example Node Names Screen



```
change node-names ip                                          Page   1 of   2
 This system is restricted to authoIP NODE NAMESor legitimate business
purposes.
    Name                IP Address
CLAN2               10.13.2.192
CMM                 10.13.2.248
default             0.0.0.0
procr               10.13.2.247




( 4 of 4 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

1. Enter the name and IP address for the C-LANs and LSPs.
2. Press **F3** (**Enter**) when complete.

Administering Network Regions

Before assigning an IP network region to a media gateway, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a media gateway with an S8300 LSP and an S8500 or S8700-series Server as the primary controller, there may be more than one network region, since there can be up to 250 media gateways of a particular type connected to the S8500 or S8700-series Server with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700-series port networks, though they may also have the same network region.

Note:

> With an S8300 or an S8400 Server, there still may be a need for more than one network region, though the S8400 supports up to five media gateways and the S8300 supports up to 50 media gateways.

A media gateway, in the case of multiple network regions, may also share the same network region as the CLAN board(s). However, it may have a different network region because of the geographic distances of the connections between the media gateway and the primary controller. The media gateway network region may also differ because of the nature of the endpoints connected to it.

To configure IP network regions for the media gateway and CLAN board(s)

CAUTION:

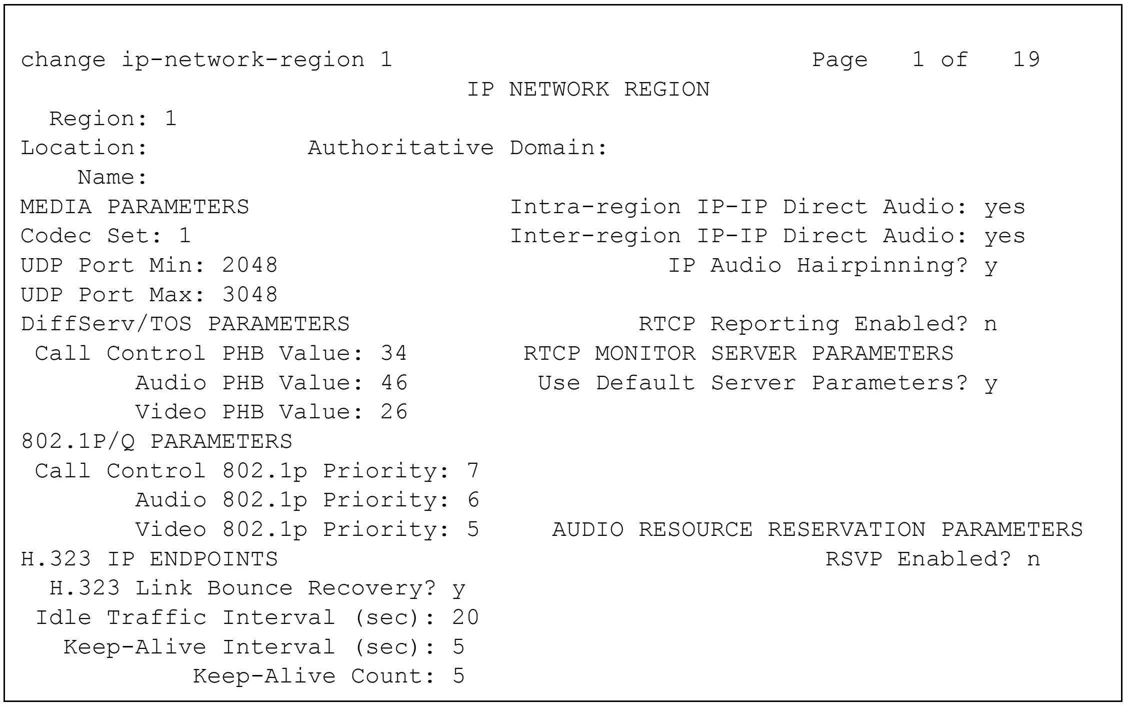
> Configuring IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

1. On the SAT screen of the primary controller for the media gateway, type **`change ip-network-region`** ***`<network_region>`***

   where ***`<network_region>`*** is the region you will assign to the media gateway. This region number may or may not match the network region of the S8400, S8500, or S8700-series CLAN boards.

   The system displays the **IP Network Region** screen.

IP Network Region Screen



```
change ip-network-region 1                             Page   1 of   19
                               IP NETWORK REGION
  Region: 1
Location:           Authoritative Domain:
    Name:
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
Codec Set: 1                      Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                           IP Audio Hairpinning? y
UDP Port Max: 3048
DiffServ/TOS PARAMETERS                    RTCP Reporting Enabled? n
 Call Control PHB Value: 34        RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46         Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

2. Complete the fields as described in *Administering Network Connectivity on Avaya Aura™ Communication Manager,* 555-233-504*.*

   Note:

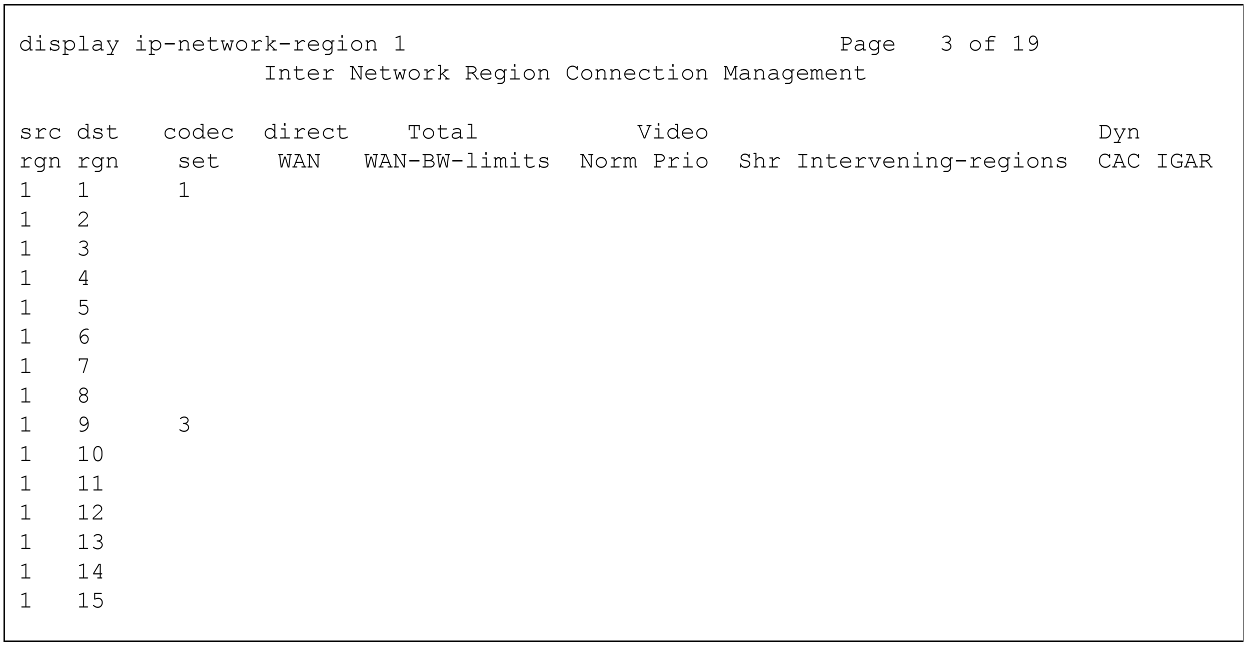
   It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. If the network region of the media gateway (1 in this example) is different from that of the S8400, S8500, or S8700-series CLAN board(s), you must interconnect the two regions.

   Press **NextPage** twice to display page 3, of the **Inter Network Region Connection Management** screen.

   This screen shows the source region (1) and the first 15 destination network region numbers. (Pages 4–19 show destination regions 16–250).

IP Network Region Screen, Page 3



```
display ip-network-region 1                              Page   3 of 19
                 Inter Network Region Connection Management

src dst   codec  direct    Total           Video                          Dyn
rgn rgn    set    WAN   WAN-BW-limits  Norm Prio  Shr Intervening-regions  CAC IGAR
1   1      1
1   2
1   3
1   4
1   5
1   6
1   7
1   8
1   9      3
1   10
1   11
1   12
1   13
1   14
1   15
```

4. Type the number for the type of codec set (1–7) that the S8400, S8500, or S8700-series Server will use to interconnect the media gateway and the C-LAN board(s) in the row corresponding to the region of the C-LAN.

   In this example, the C-LAN is in region 9 and codec-set type 3 is to be used for the interconnection between region 1 and region 9. (In this example, codec type 1 is used for communication within region 1.)

   The SAT command, **list ip-codec-set**, lists the types of codecs available on this server.

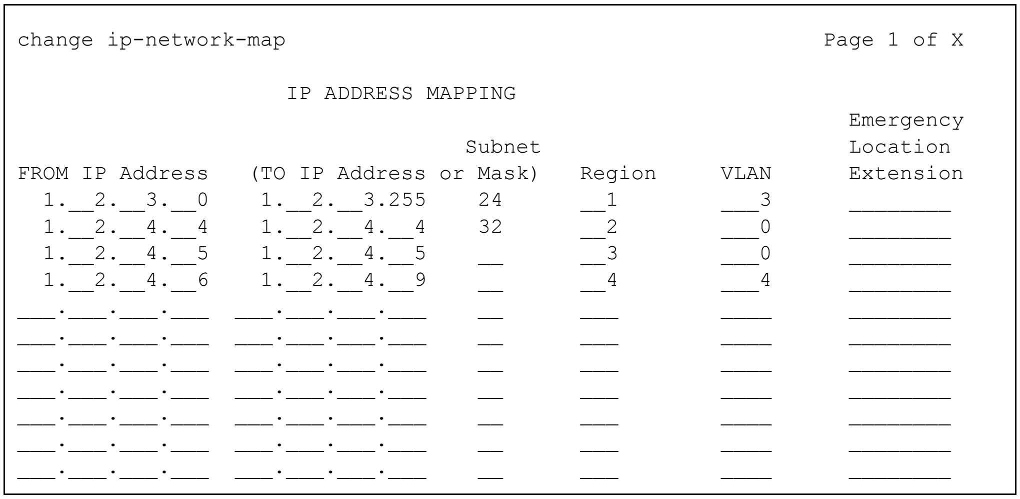
   For more detail about the Inter Network Region Connection Management form, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

5. Press **F3** (**Enter**) when complete.

Administering the IP address map

Administer the IP address map to assign IP phones and other IP endpoints to the same network region as the media gateway.

1. Type **`change ip-network-map`** and press **Enter** to display the IP Address Mapping screen.



```
change ip-network-map                                          Page 1 of X

                     IP ADDRESS MAPPING
                                                                 Emergency
                                   Subnet                        Location
FROM IP Address   (TO IP Address or Mask)   Region     VLAN      Extension
  1.__2.__3.__0    1.__2.__3.255    24      __1        ___3      ________
  1.__2.__4.__4    1.__2.__4.__4    32      __2        ___0      ________
  1.__2.__4.__5    1.__2.__4.__5    __      __3        ___0      ________
  1.__2.__4.__6    1.__2.__4.__9    __      __4        ___4      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
___.___.___.___  ___.___.___.___    __      ___        ____      ________
```

2. In the **FROM IP Address** and **TO IP Address** fields, enter a range of IP addresses for IP phones or other IP endpoints connected to the media gateway.
3. In the **Region** field, enter the network region to which the media gateway and its IP endpoints are to be assigned.
4. In the **VLAN** field, enter the VLAN number the IP endpoints should be a member of. Each network region should have its own VLAN number.
5. Enter an extension number in **Emergency Location Extension** field.

Note:

For more detail about the IP Address Mapping form, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Administering IP Interfaces

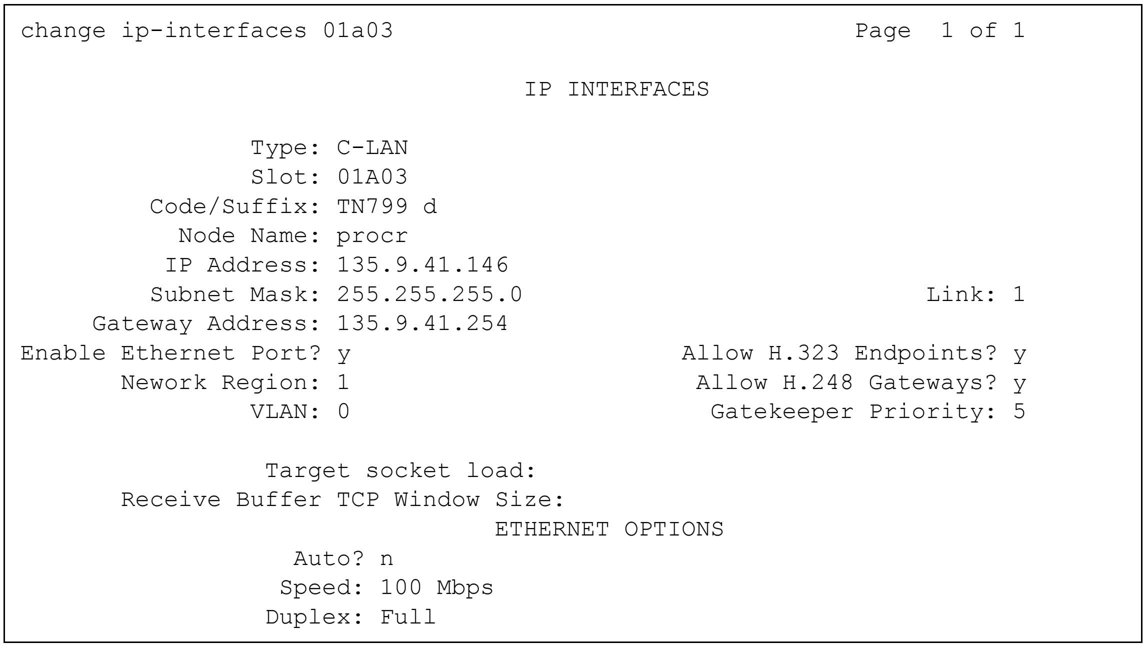
To define the IP interfaces of the S8400, S8500, or S8700-series port network CLAN boards

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Server installation.

1. Type **`change ip-interfaces`** ***`<slot location>`*** to open the **IP Interfaces** screen.

IP Interfaces Screen



```
change ip-interfaces 01a03                                Page  1 of 1

                                   IP INTERFACES

                Type: C-LAN
                Slot: 01A03
         Code/Suffix: TN799 d
           Node Name: procr
          IP Address: 135.9.41.146
         Subnet Mask: 255.255.255.0                            Link: 1
     Gateway Address: 135.9.41.254
Enable Ethernet Port? y                       Allow H.323 Endpoints? y
       Nework Region: 1                        Allow H.248 Gateways? y
                VLAN: 0                         Gatekeeper Priority: 5

                 Target socket load:
       Receive Buffer TCP Window Size:
                                 ETHERNET OPTIONS
                   Auto? n
                  Speed: 100 Mbps
                 Duplex: Full
```

2. Complete the fields as described in Table 10

Table 10: IP interfaces field descriptions

Field	Conditions/Comments
Type	Either C-LAN.
Slot	The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799 for C-LAN.
Node name	The unique node name for the IP interface. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the C-LAN.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see "*Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*".
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
	1 of 2

Table 10: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Enable Ethernet Port?	The Ethernet port must be enabled (**y**) before it can be used. The port must be disabled (**n**) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
VLAN	The VLAN number assigned to the C-LAN, if any.
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Receive Buffer TCP Window Size	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.
Link	This display only field shows the unique number for the Ethernet link. The Ethernet link was assigned on the data module form.
Allow H.323 Endpoints	Enter a ’y’ to allow H.323 endpoint connectivity on this CLAN. Enter ’n’ if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter ’y’ to allow H.248 gateway connectivity to this CLAN. Enter ’n’ if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to a yes on this form.
Auto?	Enter ’y’ or ’n’ to set auto-negotiation.
Speed	Enter 10 or 100 Mbps if **Auto** was set to no.
Duplex	Enter half or full if **Auto** was set to no.
	2 of 2

To define the IP interface of the S8400, S8500/S8510, or S8700-series Server for Processor Ethernet

Note:

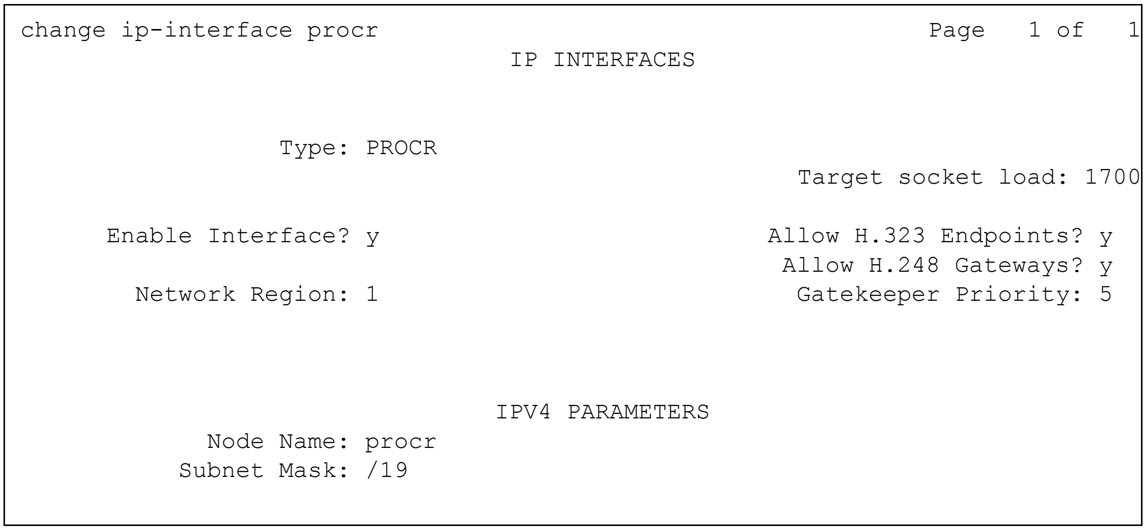
This should have already been established as a part of normal S8400 or S8500 Server installation.

1. Type **`change ip-interfaces procr`** to open the **IP Interfaces** screen.

   Note:

   If the ip-interface procr does not exist, type **`add ip-interface procr`**.

IP Interfaces Screen



```
change ip-interface procr                                       Page   1 of   1
                                  IP INTERFACES


                  Type: PROCR
                                                    Target socket load: 1700

      Enable Interface? y                         Allow H.323 Endpoints? y
                                                   Allow H.248 Gateways? y
        Network Region: 1                           Gatekeeper Priority: 5




                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /19
```

2. Complete the fields as described the in Table 11.

Table 11: IP interfaces field descriptions

Field	Conditions/Comments
Type	Display only. PROCR
Node name	The unique node name for the IP interface. **procr** is the default node name. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the Processor Ethernet.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see "*Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*".
Enable Ethernet?	The Ethernet port must be enabled (**y**) before it can be used. The port must be disabled (**n**) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
	1 of 2

Table 11: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Target Socket Load	Enter the maximum number of sockets targeted for this interface. The default is 80% of the maximum of 2500 for an S8400 Server and 3500 for an S8500 or S8700-series Server. When all the IP interfaces within the same Gatekeeper Priority exceeds the target number that you allocate, the system continues to add sockets until the interface is at its maximum capacity.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to a yes on this form.
	2 of 2

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the survivable-processor screen, their status can be viewed with the **`list survivable-processor`** command.

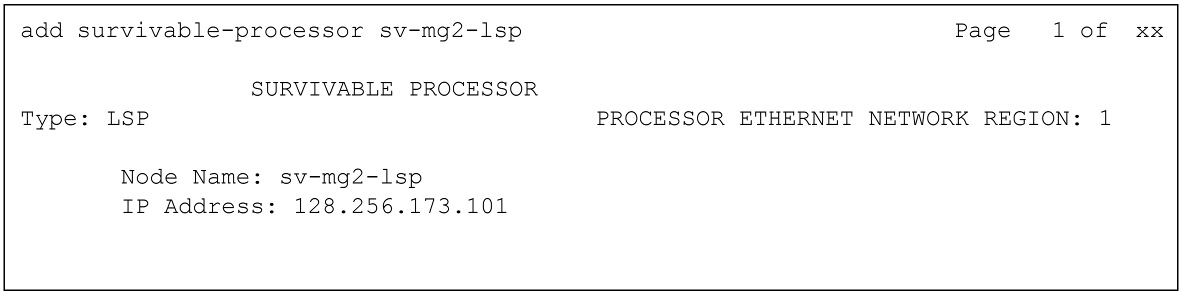
Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

1. At the SAT command line, type **`add survivable-processor`** ***`<name>,`*** where ***`<name>`*** is the LSP name from the Node Names screen.

   The Survivable Processor screen appears.

Figure 17: Add Local Survivable Processor screen



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

                SURVIVABLE PROCESSOR
Type: LSP                               PROCESSOR ETHERNET NETWORK REGION: 1

       Node Name: sv-mg2-lsp
       IP Address: 128.256.173.101
```

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Node Name is a display-only field that shows the name used to identify this server. You enter node names through the IP Node Names screen.
4. IP Address is a display-only field that shows the IP address that corresponds to the node name you entered.
5. Enter a Processor Ethernet Network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support. Valid values can be from 1 to250. Enter the network region in which the PE interface of the LSP resides.

   Note:

   With the LSP now administered on the primary controller, the LSP can register.
6. At the SAT, type list survivable-processor to verify that the LSP is registered.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **`save translation lsp`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

   Note:

   If the LSP is registered to the primary controller, the **`save translation lsp`** command transfers the super-user and other accounts from the primary controller to the LSP.

Assigning LSPs with Network Regions

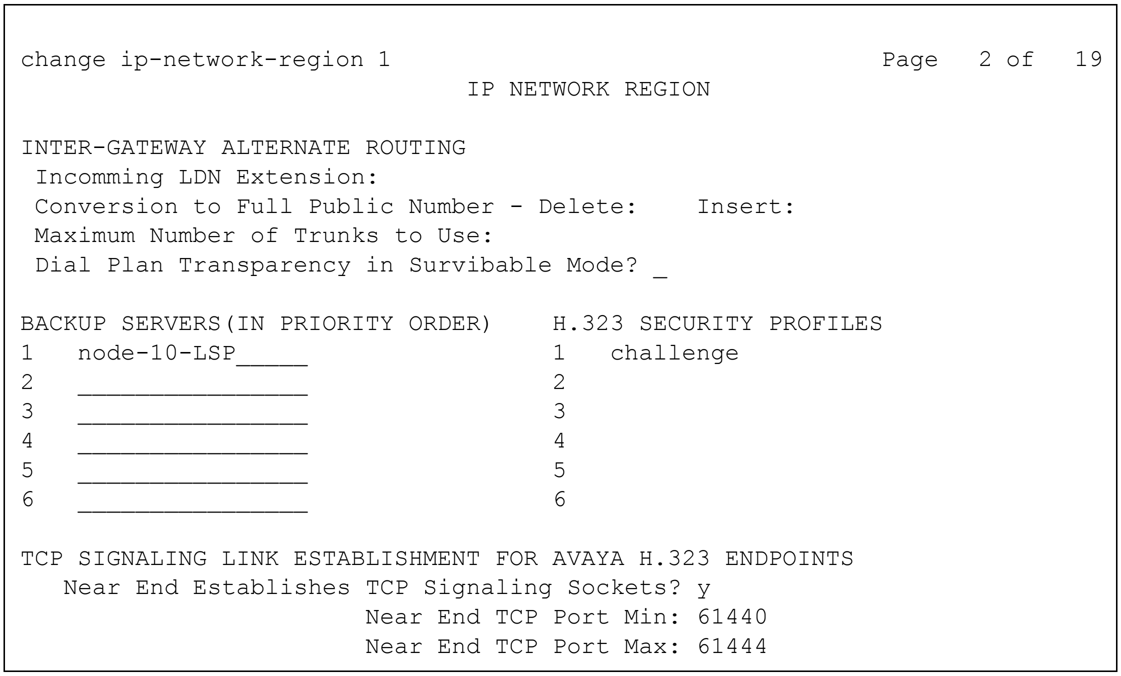
If the primary controller has LSPs, you can assign the LSPs to network regions. In the event of a network failure, IP telephones assigned to a network region will register with the LSPs assigned to that region.

This procedure assigns up to six LSPs to a network region.

To assign LSPs to a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2



```
change ip-network-region 1                                  Page   2 of   19
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING
 Incomming LDN Extension:
 Conversion to Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use:
 Dial Plan Transparency in Survibable Mode? _

BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES
1   node-10-LSP_____                 1   challenge
2   ________________                 2
3   ________________                 3
4   ________________                 4
5   ________________                 5
6   ________________                 6

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Sockets? y
                        Near End TCP Port Min: 61440
                        Near End TCP Port Max: 61444
```

2. Enter the names of up to six LSPs to be assigned to region 1.

   The LSP names must be the same as administered on the **Node Names** form.

3. Submit the form.
4. Repeat for each network region to which you want to assign LSPs.

Administering the Media Gateway

To perform the procedures in this section, SSH to the primary controller, log in, and open a SAT session.

CAUTION:

Before administering a media gateway, make sure that the gateway has been fully configured.

In this section, you will do the procedures:

- Adding a media gateway
- Verifying changes
- Enabling Announcements, if necessary
- Saving Communication Manager translations

Adding a media gateway

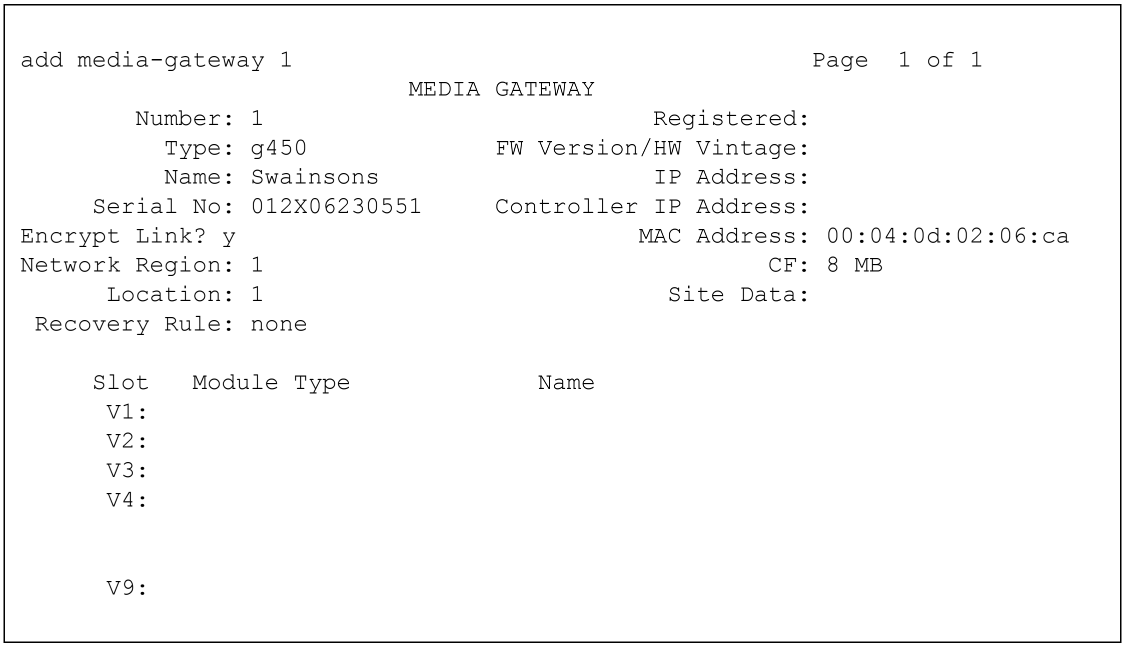
To add a media gateway:

1. At the SAT prompt, type **`add media-gateway`** ***`<number>`***

   where ***`<number>`*** is the gateway number from 1 to *n*. (*n* is 50 for an S8300, 5 for an S8400, and 250 for an S8500 or S8700-series Server).

   The **Media Gateway** screen appears.

Add media gateway Screen



```
add media-gateway 1                                        Page   1 of 1
                           MEDIA GATEWAY
        Number: 1                             Registered:
          Type: g450                FW Version/HW Vintage:
          Name: Swainsons                     IP Address:
     Serial No: 012X06230551        Controller IP Address:
Encrypt Link? y                              MAC Address: 00:04:0d:02:06:ca
Network Region: 1                                     CF: 8 MB
      Location: 1                              Site Data:
 Recovery Rule: none

     Slot   Module Type             Name
      V1:
      V2:
      V3:
      V4:


      V9:
```

2. Complete the **Name** field with the hostname assigned to the media gateway.
3. Complete the **Serial No** field with the serial number of the media gateway.

   You can obtain the serial number by typing the **`show system`** command at the MGP command line interface.

⚠ **CAUTION:**

Be sure the serial number for the media gateway you enter in this procedure matches *exactly* the serial number displayed in the **`show system`** command. The serial number is case-sensitive, and if entered incorrectly, will prevent the S8300 Server from communicating with the media gateway.

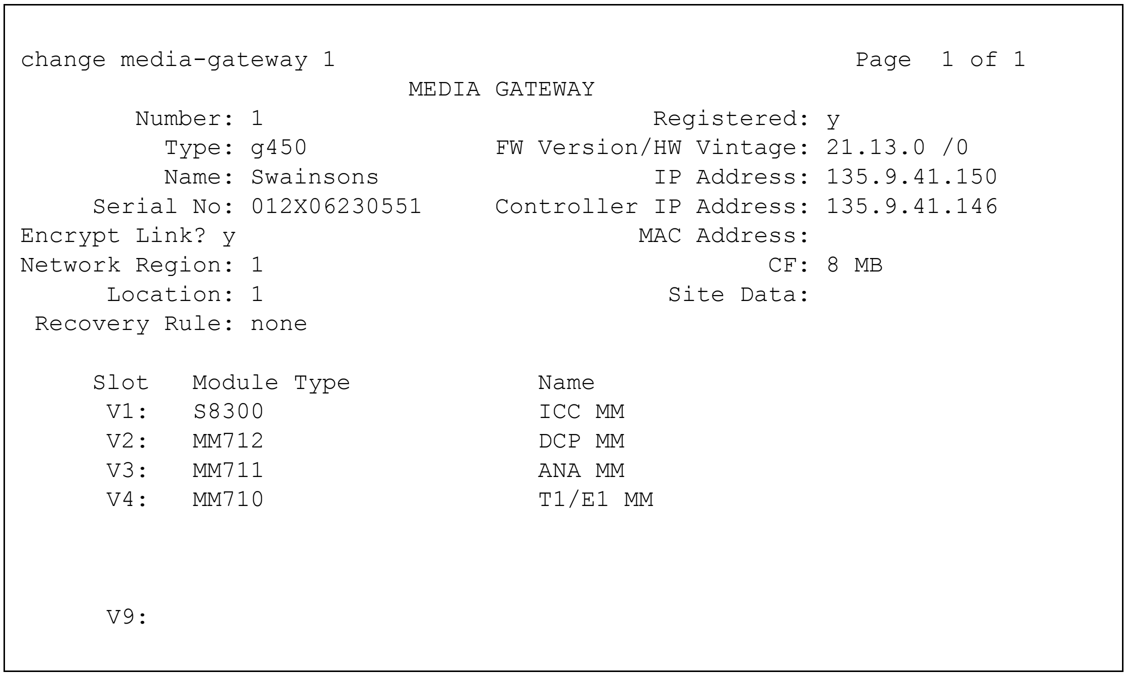
4. Complete the **Network Region** field with the value supplied in the planning documentation.
5. If specifically requested by the customer or your planning documents, type **gateway-announcements** in the V9 field.

   This field allows you to enable announcements on the media gateway. V9 is a virtual slot. There is no announcement board associated with it. The announcements for the media gateway are available in the media gateway firmware and are administered in the same way as announcements on the TN2301 circuit pack used on S8400, S8500, or S8700-series port networks.

   If there are multiple media gateways sharing announcements, then enable announcements on the media gateway whose trunks will receive the announcements most often.
6. Press **F3** (**Enter**) to save your changes.

   If properly administered, the media gateway should register with the primary controller within 1–2 minutes. The **IP Address**, **MAC Address**, and **Module Type** fields are populated automatically after the media gateway registers with the server.
7. Type `display media-gateway n`, where `n` is the media gateway number, to view the **Media Gateway** screen.

Media Gateway screen (after registration with primary controller)



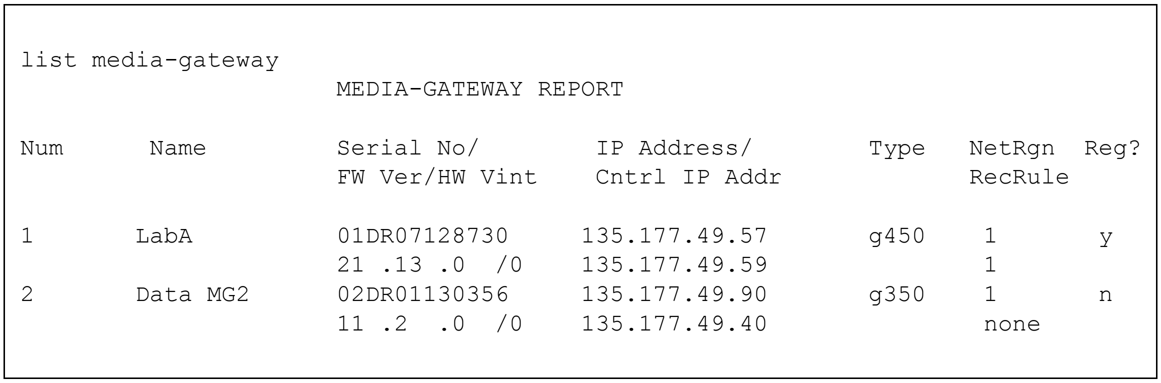
```
change media-gateway 1                                    Page  1 of 1
                           MEDIA GATEWAY
        Number: 1                           Registered: y
          Type: g450            FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                   IP Address: 135.9.41.150
     Serial No: 012X06230551     Controller IP Address: 135.9.41.146
Encrypt Link? y                            MAC Address:
Network Region: 1                                   CF: 8 MB
      Location: 1                            Site Data:
 Recovery Rule: none

     Slot   Module Type             Name
      V1:   S8300                   ICC MM
      V2:   MM712                   DCP MM
      V3:   MM711                   ANA MM
      V4:   MM710                   T1/E1 MM




      V9:
```

The media modules installed in the media gateway are listed next to their slot numbers. Verify that a media gateway has been successfully added.

Verifying changes

8. At the SAT prompt, type **`list media-gateway`**.

Media-Gateway Report screen



```
list media-gateway
                      MEDIA-GATEWAY REPORT

Num      Name         Serial No/        IP Address/        Type   NetRgn  Reg?
                      FW Ver/HW Vint    Cntrl IP Addr             RecRule

1       LabA          01DR07128730     135.177.49.57       g450    1       y
                      21 .13 .0  /0    135.177.49.59               1
2       Data MG2      02DR01130356     135.177.49.90       g350    1       n
                      11 .2  .0  /0    135.177.49.40               none
```

9. Verify that the media gateway has registered.

   The `y` in the registered field signifies that the media gateway has registered. If the should become unregistered, the `y` will become an `n`, but the IP address will remain assigned to the media gateway. If the has never been registered, the IP Address field will be blank.

   If the fails to register, two common causes are:

- The serial number administered in the **Serial No** field on the change media-gateway form is incorrect. To check, log back into the gateway and type **`show system`**. Check the serial number that appears.
- There is no IP connection between the media gateway and the S8300. To check, type **`show mgc`** and then **`ping mgp`** ***`<controller_address>`***.

Enabling Announcements, if necessary

10. *Only if specifically requested by the customer or your planning documents,* at the SAT prompt, type **`enable announcement-board`** ***`<gateway_number>`*** **`V9`**

    where ***`<gateway_number>`*** is the number of the media gateway you added.

    `V9` is the virtual slot (for example, ***`2V9`*** means media gateway number 2, slot V9.
11. Press **Enter** to enable announcements.

    The system displays the message,

    ```
    Command successfully completed
    ```

Saving Communication Manager translations

Save translations again after all Communication Manager administration is complete.

12. At the SAT prompt, type **`save translation all`**

    When the save is finished, the following message appears:

    ```
    Command successfully completed.
    ```

If using Communication Manager Messaging, administer Communication Manager for Integrated Messaging

A number of administration tasks must be performed to allow Communication Manager Messaging to work. These tasks are explained in detail in *Administering Media Servers to Work with IA770*.

CAUTION:

Communication Manager Messaging processes messages using the G.711 codec only. Therefore, ensure that a codec set exists that uses only the G.711 codec. Then, assign that codec set to a network region. And, finally, assign that network region to the Communication Manager Messaging signaling group that is linked to the Communication Manager Messaging trunk group.

Installing the authentication file to the S8300 LSP

Note:

Perform this procedure if the server you are installing is an S8300 LSP

A super-user login, dadmin, or other customer super-user login must exist on the S8300 LSP before you install an authentication file in this step. If all the configuration and administration steps have been completed and the S8300 LSP is registered to the primary controller and has successfully completed a filesync; the super-user account will automatically be copied to the S8300 LSP from the primary controller.

If you need to create a super-user login, see Creating a super-user login on the primary controller on page 224.

To install the authentication file:

1. Under **Security**, select **Authentication File**.

   The **Authentication File** screen appears.

2. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system displays the status of the installation of the the authentication file.

Administering SES

Installing the SES license

If you enabled SES, you must install the SES license from the WebLM server that is located on an edge or a combined home/edge server:

1. On the **Communication Manager System Management Interface** main page, click **SIP Enablement Services** under the **Administration** menu.

   The system opens the SIP Enablement Services screen.

2. Select **Server Configuration > License**.

   The **List Licenses** page displays.

3. Click **Access WebLM**.

   The **WebLM** application screen displays in a new window.

4. If this is the first time the application has run, you must log in with *admin* as the default login and *weblmadmin* as the default password, then change both the default login and password to the customer's preferences for this account.

   Note:

   > If the WebLM server is on a different subnet than the server, you must change the URL in your browser to include the server's DNS name. When you mouse-over the WebLM link on the List Licenses page, the URL includes an IP address, for example, "https://12.34.56.78/WebLM/index.jsp/." Change the URL to "https://*server-name*/WebLM/index.jsp/," where *server-name* is the DNS name of the server on which you want to install the SES license.

5. Select **License Administration**.

   The authentication screen appears.

6. Login as *admin* and enter the password.

   After this initial login, the system prompts you to change the password.

7. Change the password.

   WebLM logs you out.

8. Log in again as *admin* with the newly-created password.

   The **Web License Manager (WebLM)** screen appears.

9. Select **Install License**.

   The **Install License** page displays.

10. Click **Browse** to navigate to the SES license that you want to install.

11. Click **Install**.

    If the license is valid, the system indicates that it was installed successfully; otherwise the process fails with a brief description.

    Note:

    > The license update for the home seats can take up to 15 minutes. Wait approximately 15 minutes before continuing with verifying the license installation (Step 12).

12. To verify the license installation go to the Integrated Management SIP Server Management **Top** page and select **Server Configuration > License**.

    The **List Licenses** page displays.

13. Ensure that the following three (3) licenses are listed in the **Name** column:

    - Edge Proxy
    - Basic Proxy
    - Home Seats

14. Click **Show** by the Edge Proxy listing.

    The **License Information** page displays.

15. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   1
    Acquired    1
    ```

16. Click **Show** by the Basic Proxy listing.

    The **License Information** page displays.

17. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   1
    Acquired    1
    ```

18. Click **Show** by the Home Seats listing.

    The **License Information** page displays.

19. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   XXX
    Acquired    XXX
    ```

    where `XXX` is the actual number of seats in the license.

20. Reboot the server:

    a. Click **Shutdown Server** under the Server heading.

    b. Select **Delayed Shutdown and Restart server after shutdown**.

    c. Click **Shutdown**.

    You will be logged off the server when it reboots. You can use ping to verify when the server is accessible again.

SES administration tasks

If you enabled SES, you must complete the following tasks to administer SES. For more information, see *Administration of SIP Enablement Services on the S8300 Server*.

1. Prepare Communication Manager.
2. Administer SIP trunks.

3. Administer call routing.
4. Administer SCCAN, if desired.
5. Administer Redirect Call Off-Net, if desired.
6. Complete the following SES Setup screens.
   - **Edit System Properties** screen, which you use to set up the SIP domain
   - **Add Host** screen, which you use to define the other servers for SES
   - **Edit Default User Profile** screen, which you use to enter location information to be assigned to each user on the local server
   - **Add Media Server** screen, which you use to define the S8300 as a host running Communication Manager
   - **Set up Master Administration** screen, which you use to define the server for storage of the main SES database
   - **WEbLM** screen, which you use to install the SES license.

Considerations for IP Phones Supported by a Local Survivable Processor

A DHCP server assigns IP addresses to IP endpoints dynamically. Avaya IP phones perform a DHCP discover request to receive an IP address, as well as receive parameters necessary to function correctly. These parameters include the location of the call control server, the location of the TFTP server, as well as the directory on the TFTP server from which the phone receives its upgrades.

When preparing a DHCP server to work with Avaya IP phones, there is an option that must be administered to allow the Avaya phone to receive the DHCP offer. This option is "site-specific-option-number" (sson) 176. Different DHCP servers allow for this administration in different ways, but the sson option must be mapped to 176. Then the option can be set up to send the information desired to the Avaya phones for the intended activity.

The sson option sends a string that includes the IP address of the Avaya Call Controller with which the phone will register ("MCIPADD=www.xxx.yyy.zzz"). In an S8400, S8500, or S8700-series system, this can be a CLAN address; in an S8400 or S8500, this can also be the IP address for the server's port that is enabled for processor ethernet; in an S8300 system, this is the IP address of the S8300. Multiple addresses can be administered to allow for LSP failover. The second address in the MCIPADD list may be an IP address for a second CLAN board or an LSP. If a second CLAN board is used, then the third address must be the LSP, and any subsequent addresses should be alternate LSPs. Local LSPs should appear first in the list, with remote LSPs later in the list as possible back ups.

If an IP phone looses its connection to the primary controller, it will try to register with an LSP associated with its network region (as defined on page 3 of the IP Network Region form). However, if the phone resets, it looses this information and goes to the DHCP server for a controller. If the only controller in the MCIPADD list is the primary controller, and if the connection to the primary controller is down, the phone cannot register. Having an LSP in the MCIPADD list gives the IP phones an alternate controller in this situation.

Note:

It is strongly recommended that at least one LSP be administered in the MCIPADD list.

Also included in the sson option string is the "MCPORT=1719". This is the port the phone will listen on for signalling traffic to the call controller. Next is the tftp server field. This field indicates to the phone where it is to receive firmware service packs, along with the tftp directory field.

All phones for which the DHCP server has an LSP as the second address in the MCIPADD list should be administered to be in the same network region. Or, if administered to be in different network regions, the network regions involved should be interconnected. Use the ip-network-map form on the primary controller to put the IP phones in the same network region. On the ip-network-map form, a range of IP addresses (or a subnet) can be specified to be in a single network region. Enter the IP address range, or subnet, that contains the IP addresses of the IP phones and enter the desired network region number for that address range. The same address range or subnet must then be administered on the DHCP server. If it is not desired that all the phones be in the same network region, the form “ip-network-region #” should be used to interconnect all the network regions that contain those phones.

Transition of Control from Primary Controller to LSP

When the network connection between a media gateway and the S8300, S8400, S8500, or S8700-series primary controller goes down, control of endpoints connected to a media gateway goes to the next point in the primary controller list, which will be either a second CLAN board or the LSP. At this point, the primary controller alarms to notify the customer and services personnel that the network connection between the primary controller and media gateway has problems. If control passes to the LSP, the LSP’s license allows it to support the media gateway endpoints for up to 30 days, within which the network problems should be resolved.

The customer may pass control back to the S8300, S8400, S8500, or S8700-series primary controller manually, by selecting **Shutdown this server** from the S8300 web page (includes selecting the option to restart after shutdown), or a technician must run **`reset system 4`** from the Linux command line. When the system reboots, the media gateway and its endpoints reregister with the primary controller.

The customer may also choose to administer Communication Manager on the System Parameters Media Gateway Automatic Recovery Rule screen, such that the primary controller accepts control back from the LSP as soon as possible, based on whether there are calls active or what time of day it is. See *Administering Avaya Aura™ Communication Manager,* 03-300509.

Split registration solution

The main server (Communication Manager) attempts to ensure the devices in a network region register to the LSP when administered to force telephones and gateways to active LSPs. This solution keeps branch-oriented operations intact with local trunk resources. LSPs turn active once a media gateway registers itself.

For example,

- A server failure activating LSPs disables all network regions served by the LSPs.
- The main server blocks future registrations of media gateways and telephones.

- The main server disables media gateways and telephones already registered with the LSPs.

Sequence of events

Administrator forces media gateways and telephones to active LSPs. The main server resets or the network fragments, causing a media gateway to unregister.

The following sequence of events occurs:

1. The media gateway registers to an LSP turning the status active.
2. The LSP reports the active status to the main server.
3. The main server unregisters all media gateways and telephones from itself. These network resources are administered for the LSP under the heading "BACKUP SERVERS" on the IP Network Region screen. These end points do not re-register on the main server.
4. The main server decides the time-day-window, scheduled to enable the endpoints to re-register or the enable mg-return command is executed.

Network Region type description

An LSP is administered as backup server for one or more network region forms. The LSP can have resources from one or more network regions (group). On implementing the split registration feature, the network regions status changes to auto-disable (ad). On reaching the Time-of-Day or executing enable mg-return command, the network regions are automatically enabled and the telephones and media gateways can register.

On executing the disable nr-registration command, network region status changes to manually disabled (rd). The administrator changes this status by executing the enable nr-registration command.

All network regions in a group are manually disabled (rd) when one or more network regions in the group have the status as rd. On activating an LSP in a group having manually disabled network regions, the auto disable (ad) code is activated. It searches for manually disabled (rd) status. Since some network regions in the group already have the manually disabled (rd) status, all network regions display the rd status.

Set Up SNMP Alarming on the media gateway

Setting up SNMP alarm reporting involves two main tasks:

- Configuring the primary server to report alarms to a services support agency
- Configuring the media gateway to send its traps to a network management system (NMS)

Configuring the primary server to report alarms to a services support agency

The primary server may be an S8300, S8400, S8500, or S8700/S8710/S8720 Server. The S8300 Server supports two methods for reporting alarms. Either, both, or no alarm-reporting method may be used at a given site.

- OSS Method.

  The server's software applications and hardware devices under its control can generate Operations Support System (OSS) alarms. These alarms are recorded in the server logs, and may be reported to Avaya's Initialization and Administration System (INADS), or another services support agency over the server's modem interface.

  To provide OSS alarm notification, the server requires a USB connection to a modem that is connected to an analog line. The modem must be configured using the S8300 Server's Web Interface, in the **Set Modem Interface** screen, and enabled to send and receive calls using the **Enable/Disable Modem** screen.

  Note:

  > Configuration of the OSS alarming method can only be done using Linux shell commands.

- SNMP Method

  SNMP traps may be sent in User Datagram Protocol (UDP) to a corporate network management system (NMS) using the **Configure Trap Destinations** screen on the S8300 Server's Web Interface. The OSS and SNMP alarm-notification methods operate independently of each other; either or both may be used. Currently, the following NMSs are supported:

  - Avaya Fault and Performance Manager, as a standalone application, or integrated within Avaya Network Management Console with VoIP SystemView
  - Avaya Network Management Console with VoIP SystemView
  - HP Openview

  To provide SNMP alarm notification, on the server Web Interface use the **Configure Trap Destinations** screen to set up SNMP destinations in the corporate NMS.

Administering INADS phone numbers and Enabling alarms to INADS

The following procedure, using the primary server's Linux shell commands, administers the dial-out modem to send alarms in the OSS method. In this example, the primary server is an S8300, and the services support agency is Avaya's Initialization and Administration System (INADS).

Perform this task after all Communication Manager administration is complete.

Note:

Do these steps only if the S8300 is the primary controller and the customer has a maintenance contract with Avaya. Use the information you acquired from the ART tool (see Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary on page 216).

Also, a USB modem must have already been installed.

To add INADS phone numbers and Enable alarms to INADS

1. With a direct connection to the S8300 Services port, open a telnet session and log in as *craft* (or *dadmin*).
2. At the Linux prompt, type **`almcall -f`** ***`INADS phone number`*** **`-s`** ***`<second-number>`*** and press **Enter**.
3. At the prompt, type **`almenable -d b -s y`** and press **Enter**.
4. Type **`almenable`** and press **Enter** to verify that the alarms are enabled.
5. Log off.

Configuring the media gateway to send its traps to a network management system (NMS)

Please refer to the appropriate gateway documentation to know the commands you need to configure the media gateway to send traps to a network management system.

Complete the Installation of the S8300 (if the Primary Controller)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process is to:

- Connect and administer test endpoints
- Test the endpoints
- Administer Communication Manager for trunks, features, networking, or other items required by the customer
- Complete the electrical installation
- Enable adjunct systems

Note:

Follow the existing process and procedures to register the S8300.

Reboot the server

To instate the foregoing administration and provisioning:

1. On the **Server (Maintenance)** Web page, select **Server > Shutdown** server.

   The **Shutdown This Server** page displays.

2. Select **Delayed Shutdown** and check the **Restart server after shutdown** box.
3. Click **Shutdown**.

Integrity check

After the server comes up verify the following:

1. Ping the IP address of the server and ensure connectivity.
2. On the **Server (Maintenance)** Web page, select **Server > Status Summary**.

   The **Status Summary Page** displays.

3. Verify the following:
   - **Mode** is **Active**.
   - **Server Hardware** is **okay**.

- **Processes** is **okay**.

4. At the Maintenance Web Pages, select **Server > Process Status**.

   The **Process Status** page displays.

5. In the Content section, select **Summary**.
6. In the Frequency section, select **Display once**.
7. Click **View**.

   The **View Process Status Results** page displays.

8. Verify that all processes are **UP**.

Updating Communication Manager Messaging, if installed

Stopping Communication Manager Messaging, if loading an Communication Manager Messaging update

After the upgrade is complete, perform the following post-upgrade tasks.

1. On the **Server (Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, under **Utilities**, select **Stop Messaging**.

   The **Stop Messaging Software** Web page is displayed.

3. Select the **Stop** button.

   The shutdown of the messaging server will begin when all users have logged off from Communication Manager Messaging or after three minutes have passed, whichever event comes first. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing Communication Manager Messaging service pack (or RFU) files, if any

If Communication Manager Messaging is being used, a post-upgrade service pack for Communication Manager Messaging may be required. See the Communication Manager Messaging documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at http://support.avaya.com.

1. Select **Messaging Administration** from the main menu.
2. Under **Software Management,** select **Adv Software Installation**.

3. Select **Continue this operation without current system backup**.
4. Select the Communication Manager Messaging update package and click **Install Selected Packages**.

   Note:

   The system automatically prompts you to restart Communication Manager Messaging when the service pack has been installed. Therefore, if you restart Communication Manager Messaging at this time, you do *not* need to perform the following procedure, Starting Communication Manager Messaging.

Starting Communication Manager Messaging

⚠ **CAUTION:**

You do *not* need to perform this task if you restarted Communication Manager Messaging as a part of the installation of the Communication Manager Messaging service pack.

After the Communication Manager Messaging application has been updated, you must restart it using the following steps:

1. On the **Server (Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.
2. From the **Messaging Administration** Web page, under **Utilities**, select **Start Messaging**.

   The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.
3. When the message `End start_vm: voice messaging is now completely up` is displayed, close the Messaging Administration Web page and do the next procedure in this document.

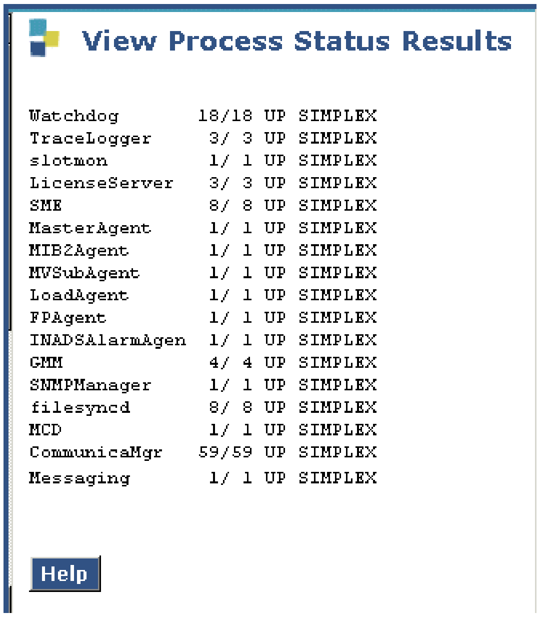
Verifying start up of Communication Manager Messaging

To verify operation of Communication Manager Messaging, perform the following steps:

1. On the **Server (Maintenance)** Web page, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

   The **View Process Status Results** screen appears.

View Process Status screen



View Process Status Results

```
Watchdog        18/18 UP SIMPLEX
TraceLogger      3/ 3 UP SIMPLEX
slotmon          1/ 1 UP SIMPLEX
LicenseServer    3/ 3 UP SIMPLEX
SME              8/ 8 UP SIMPLEX
MasterAgent      1/ 1 UP SIMPLEX
MIB2Agent        1/ 1 UP SIMPLEX
MVSubAgent       1/ 1 UP SIMPLEX
LoadAgent        1/ 1 UP SIMPLEX
FPAgent          1/ 1 UP SIMPLEX
INADSAlarmAgen   1/ 1 UP SIMPLEX
GMM              4/ 4 UP SIMPLEX
SNMPManager      1/ 1 UP SIMPLEX
filesyncd        8/ 8 UP SIMPLEX
MCD              1/ 1 UP SIMPLEX
CommunicaMgr    59/59 UP SIMPLEX
Messaging        1/ 1 UP SIMPLEX
```

3. Make sure Messaging shows **UP**.

   The number of processes (59/59) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 58/59 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an Communication Manager Messaging sanity test:

   a. At the Linux command line, type **`/vs/bin/display`**.

   b. Verify that all states are `Inserv`.

6. At the Linux command line, type **`/VM/bin/ss`**.
7. Verify that all Communication Manager Messaging processes are shown.

If Communication Manager Messaging fails to start after a new installation

If you have installed or upgraded Communication Manager Messaging and it does not start, you must ensure that an IP address has been provided for use with Communication Manager Messaging. To check for the IP address, you must use the **Configure Server** option on the Communication Manager System Management Interface.

On the Configure Interfaces screen, ensure that a valid IP address is present in the **Integrated Messaging** section**.**

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **`save translation all`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

Backing up system data

You can back up the S8300-Series Server data by:

- Backing up the system to compact flash media on page 282
- Backing up the system over the customer's LAN on page 283

Backing up the system to compact flash media

S8300C Server allows back up using a compact flash card.

To back up the system to compact flash media

1. Plug the cable to the compact flash drive into a USB port on the S8300C Server.
2. Insert a 128-Mb compact flash media into the card reader or writer.
3. On the **Server (Maintenance)** Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.
4. In the Data Sets section select all of the following data sets:
   - If the S8300B, S8300C, or S8300D Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - If Communication Manager Messaging is installed on the S8300B, S8300C, or S8300D Server, select **Translations, Names and Messages**.

Note:

Depending on the customer's Communication Manager Messaging configuration, the back up size of the Communication Manager Messaging data set (**Translations, Names and Messages)** can be larger than the size of the compact flash drive (maximum size of the compact flash drive is 128 MB).

5. Select the Backup Method:
   - Local PC Card
6. Optionally, select **Format Compact Flash** to format a new card.

   Note:

   The compact flash card needs to be formatted only before the first use.
7. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

Backing up the system over the customer's LAN

To back up the data on an S8300 Server:

1. On the **Server (Maintenance)** Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.
2. In the Data Sets section select all of the following data sets:
   - If the S8300B, S8300C, or S8300D Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - If Communication Manager Messaging is installed on the S8300B, S8300C, or S8300D Server, select **Translations, Names and Messages**.
3. Select the Backup Method:
   - Network Device: enter the customer-supplied information for:
     - User Name

       You must enter a valid user name to enable the S8300 Server to log in to the FTP, SFTP, or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.
     - Password

       You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP site may have a different convention.

- Host Name

  Enter the DNS name or IP address of the FTP, SFTP, or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

- Directory

  Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. If you do not want to use the default directory, you must enter the full path from the ftp server root.

4. Click **Start Backup**.

   Wait for the message indicating that the backup was successful.

5. To check the status of the backup:

   a. Under **Data Backup/Restore**, click **Backup History**.

   b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

      When the backup is finished, the **Backup History Results** screen displays the following message:

   ```
   The final status for your backup job is shown below
   ```

   For each backup set, the following message is displayed if set was backed up successfully:

   ```
   BACKUP SUCCESSFUL
   ```

   ⚠ **Important:**
   When you do full back up, Communication Manager Messaging data is not backed up.

6. If Communication Manager Messaging is installed on the S8300A , S8300B, S8300C, or S8300D back up announcements:

   - Return to the **Backup Now** screen and uncheck all but **Announcements**.
   - Select the Backup Method (see Step 3 above).
   - Click **Start Backup**.

Complete the Installation Process (for an S8300 LSP)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test endpoints

This completes the installation of the a media gateway with an S8300 LSP.

Final tasks

Perform the following tasks to complete the server installation:

1. On the **Server (Maintenance)** Web page, select **Server > Status Summary** and check the overall health of the system.
2. Resolve any alarms (**Alarms > Current Alarms**).
3. Save translations (**Data Backup/Restore > Backup Now**).
4. Set backup schedules (**Data Backup/Restore > Schedule Backup**).
5. At the server command line type **`productid -p`** ***`product_id`*****,** where ***`product_id`*** is the product ID you received from the customer or the ART tool.
6. Re-enable alarm origination:
   a. At the server command line type **`almenable -d b -s y`** and press **Enter**, where:
      - **`-d b`** sets the dialout option to both numbers
      - **`-s y`** enables sending SNMP traps.

   b. Type **`almenable`** without any options and press **Enter** to verify that alarm origination is enabled.
7. Logoff the system.

Chapter 6: Manual upgrade of an existing S8300B or S8300C to Release 5.2

This chapter covers the procedures to upgrade the software on an installed Avaya S8300B or S8300C Server from release 2.x, 3.x, or 4.x to release 5.2.

For procedures to upgrade the media gateway that contains the S8300 Server, refer to the appropriate gateway documentation. This chapter also covers the procedures to upgrade the firmware on an installed media gateway.

⚠ **Important:**

This chapter assumes that the currently installed S8300 is version B or C. The S8300B runs Communication Manager release 2.0 or greater. The S8300C runs Communication Manager release 4.0 or later. If the currently installed S8300 is version A, follow the upgrade procedures in Chapter 7: Migrating an S8300 Server on page 351.

Considerations for upgrading the S8300B or S8300C as a primary controller or as an LSP

The S8300 can be configured as either the primary controller or as a local survivable processor (LSP). When the S8300 is an LSP, the primary controller, running Communication Manager, can be either another S8300 or an S8400, S8500-Series, or S8700-Series Server.

> ⚠ **CAUTION:**
>
> When you are upgrading the S8300 Server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the S8300 Server to a release that is not supported as an upgrade path, you might corrupt the translations.
>
> Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.
>
> To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access http://support.avaya.com. Select **Downloads** > **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates** > **Latest Communication Manager Software & Firmware Compatibility Matrix**.

The steps to manually upgrade an S8300 configured as an LSP are the same as the steps to upgrade an S8300 configured as the primary controller, with the following additional considerations:

- The version of Communication Manager running on the LSP must be exactly the same as, or a later version that is compatible with, the version running on the primary controller.
- If upgrading both the primary controller and the LSP to the same release, you must upgrade the LSP first. Next, you upgrade the media gateways, including the media gateway that houses the primary controller, if the primary controller is an S8300. Then, with Communication Manager turned off on the LSP, you upgrade the primary controller.
- An LSP *cannot* have SIP Enablement Services (SES) enabled.
- An LSP must be configured as XL if the primary controller is an S8720 Server in an XL configuration or an S8730 Server. Administer this option on the Configure Server — Configure LSP Web page.

Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323 on an S8300B Server

⚠ **CAUTION:**

Communication Manager Release 5.2 does not support the CWY1 integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300B Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current IA770 integration administration before the upgrade and then administer the integration to H.323 after the upgrade.

For instructions on converting the integration to H.323, including the removal of existing administration, see *Administering Media Servers to Work with IA770*.

⚠ **CAUTION:**

Be sure to test the new integration before completing the upgrade.

The need to restore IP phone files

During an upgrade, any data in the /tftpboot directory is overwritten with new software and firmware. If the system was using the http or tftp capability for 4600-series phone firmware downloads and configuration updates, the firmware and 4600-series phone configuration files are overwritten.

You must retrieve the 46xx firmware (the 46xx .tar file, for example **46xxH323_cm2_2_wi1_15_ipt2_2_111405.tar**) from the Avaya Downloads Web site and download the 46xx firmware file to the server after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the /tftpboot directory *after* the upgrade. See the following:

- Saving a copy of the 4600-series telephone configuration file, if any on page 311
- Copying IP Phone firmware to the server, if necessary on page 343
- Installing IP phone firmware download configuration file on page 343

Tasks to upgrade the S8300B or S8300C to release 5.2

The major tasks to upgrade the S8300B or S8300C to release 5.2 are:

Before going to the customer site

- Obtaining a USB DVD/CD-ROM drive on page 292

- Obtaining the serial number of the media gateway, if necessary on page 292
- Checking the number of allocated ports, if the S8300 Server is a primary controller on page 292
- Checking the availability of the FTP, SFTP, or SCP server for backing up data on page 292
- Obtaining S8300 software on page 293
- Obtaining service pack files on page 294
- Obtaining service pack and language files for the messaging application, if necessary on page 296
- Completing the RFA process (obtaining license and authentication files) on page 298
- Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary on page 299

On-site Preparation for the Upgrade

- Accessing the S8300 on page 300
- Ensuring a super-user login exists on page 300
- Creating a super-user login, if one does not exist (releases earlier than Release 4.0) on page 302
- Creating a super-user login, if necessary (release 4.0 or 4.0.x only) on page 303
- Copying a pre-upgrade service pack file to the S8300 Server on page 307
- Removing the administration for the IA770 integration if CWY1 board is used on page 307
- Completing pre-upgrade tasks — if the target S8300 is the primary controller on page 308
- Saving a copy of the 4600-series telephone configuration file, if any on page 311
- Getting IA770 data and Stopping IA770 (if IA770 is being used) on page 311
- Backing up data on the S8300 Server on page 316
- Copying and installing the service pack files to the S8300 Server (starting from R2.x or from R4.x only) on page 320
- Copying Files to the S8300 hard drive on page 322
- Copying the software and firmware files to the server on page 323

Upgrade the S8300

- Installing new software on page 329
- Installing updated Communication Manager license and authentication files on page 333
- If upgrading an S8300C LSP, configuring the LSP for compatibility with an XL configuration on page 335
- If the server is an LSP, stop and start Communication Manager on page 335

- In the Memory Config field, verify that the setting is Extra Large.If on page 336
- Installing security updates, Communication Manager service pack updates, and SES service pack updates, if any on page 336
- If Communication Manager Messaging has been upgraded, verify messaging has started on page 339
- Testing to verify system functionality on page 341
- Making the upgrade permanent on page 341
- Saving translations on page 342
- If Communication Manager Messaging fails to start after an upgrade on page 342
- Copying IP Phone firmware to the server, if necessary on page 343
- Installing IP phone firmware download configuration file on page 343

Upgrade the Firmware on a Media Gateway

- Upgrading the Firmware on a Media Gateway on page 344

Post-upgrade tasks

- Stopping Communication Manager Messaging, if loading an Communication Manager Messaging update on page 345
- Installing Communication Manager Messaging service pack (or RFU) files, if any on page 345
- Starting Communication Manager Messaging on page 346
- Verifying start up of Communication Manager Messaging on page 346
- Saving translations on page 347
- If using Communication Manager Messaging, administering switch integration for H.323 on page 348
- Testing to verify system functionality on page 348
- Completing the upgrade process (S8300 is the primary controller) on page 348
- Backing up the system on page 350

Before going to the customer site

The procedures in this section should be completed before going to the customer site or before starting a remote installation.

Obtaining a USB DVD/CD-ROM drive

Upgrading Communication Manager on an S8300 requires downloading Communication Manager software files from an external USB CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD/CD-ROM drive at the site.

Obtaining the serial number of the media gateway, if necessary

To get the serial number of the media gateway, ask the customer's administrator to:

1. Log in to the S8300 Maintenance web pages.
2. Select **View License Status** or **License File** from the main menu to display the serial number.

Checking the number of allocated ports, if the S8300 Server is a primary controller

Note:

Skip this section if the S8300 Server is an LSP.

With the S8300 Server as a main server, the maximum number of ports is 900.

⚠ **CAUTION:**

If the maximum number of ports exceeds 900 for an S8300 Server as a main server, there may be a problem with the upgrade and you need to escalate the issue to your Project Manager.

To check the system for the maximum number of ports, ask the customer to:

1) Log in to the SAT screen.

2) At the SAT command, display `system-parameters customer-options`.

3) Verify that the **Maximum Ports:** field is 900 or less.

Checking the availability of the FTP, SFTP, or SCP server for backing up data

Before you begin the upgrade procedure, you can back up the system data to an FTP, SFTP, or SCP Server over the customer's LAN or to a USB Compact Flash card. The option to back up to an SCP or an SFTP server is available only with Communication Manager release 3.1 and later.

A current version of the system data is required to restore the system configuration upon completion of the migration.

- Check with your project manager or the customer for the following information about the FTP Server (Back up on a SFTP, or SCP Server is limited to a few releases):
  - Login ID and password
  - IP address
  - Directory path on the FTP Server

⚠ **Important:**
Before going to the customer site, make sure that you can use a customer server over the LAN for back ups.

Note:
(S8300C only) You can use an external Avaya approved Compact Flash card and a Card Reader to do the back up.

Obtaining S8300 software

The files containing the software for the S8300 and the media gateway module firmware are on the Communication Manager Software Distribution CD-ROM that you take to the site. This CD is called the software CD because it contains software for all of the Linux servers. SIP Enablement Services (SES) and Communication Manager Messaging software (starting with Communication Manager release 5.2, IA770 Intuity Audix application is called Communication Manager Messaging software) is also stored on the Communication Manager Software Distribution CD-ROM.

Additional files that may be needed are:

- Post-upgrade Communication Manager software service pack
- License files (for Communication Manager, and optionally, for SES)
- Avaya authentication file
- New firmware files
- Security updates
- Communication Manager Messaging service packs, RFUs, announcement files, or language sets

Obtaining service pack files

Pre- and post-upgrade service packs may be needed for this upgrade. If the service pack files are not on your software CD, download the service pack files from the Avaya Support web site to your laptop.

⚠ **Important:**

To determine if the current software release needs a pre-upgrade patch, visit, http://support.avaya.com/japple/css/japple?temp.documentID=361270&temp.productID=136527&temp.releaseID=348072&temp.bucketID=108025&PAGE=Document. On the Web page, you can find the upgrade patch under **Pre-Installation Software**.

Pre-upgrade service pack (starting from R2.x only)

This upgrade requires a pre-upgrade service pack. The service pack filename differs, depending on which software load the media server is using. See Table 12: Pre-Upgrade service pack filenames for software release and load for the software load associated with each release.

⚠ **CAUTION:**

If the customer’s system has Release 2.x of Communication Manager but has a field load other than those listed in the table, do not use this section to upgrade Communication Manager to Release 3.0 or later releases. You must escalate the issue to your project manager.

Table 12: Pre-Upgrade service pack filenames for software release and load

Software release of existing media server	Associated software load	Service pack filename
Release 2.0	R012x.00.0.219.0	00.0.219.0-xxxx.tar.gz
Release 2.0.1	R012x.00.1.221.1	00.1.221.1-xxxx.tar.gz
Release 2.1	R012x.01.0.411.7	01.0.411.7-xxxx.tar.gz
Release 2.1.1	R012x.01.1.414.1	01.1.414.1-xxxx.tar.gz
Release 2.2	R012x.02.0.111.4	02.0.111.4-xxxx.tar.gz
Release 2.2.1	R012x.02.1.118.1	02.1.118.1-xxxx.tar.gz
Release 2.2.2	R012x.02.2.122.0	02.2.122.0-xxxx.tar.gz

Pre-upgrade service pack (starting from R4.0 on an S8300C only)

Note:

Skip this task if the release running on the S8300C is R4.0.1 or later. Perform this task only if you are upgrading an S8300C Server from R4.0 to a later release.

An upgrade from R4.0 to R5.2 on an existing S8300C requires you to first install a pre-upgrade service pack.

To locate the pre-upgrade service pack:

1. Visit http://support.avaya.com/japple/css/japple?temp.documentID=361270&temp.productID=136527&temp.releaseID=348072&temp.bucketID=108025&PAGE=Document.
2. In the **Pre-Installation Software** section, locate the pre-upgrade or pre-installation patch for Communication Manager release 4.0 to 5.2 for an S8300C Server.

Post-upgrade service pack

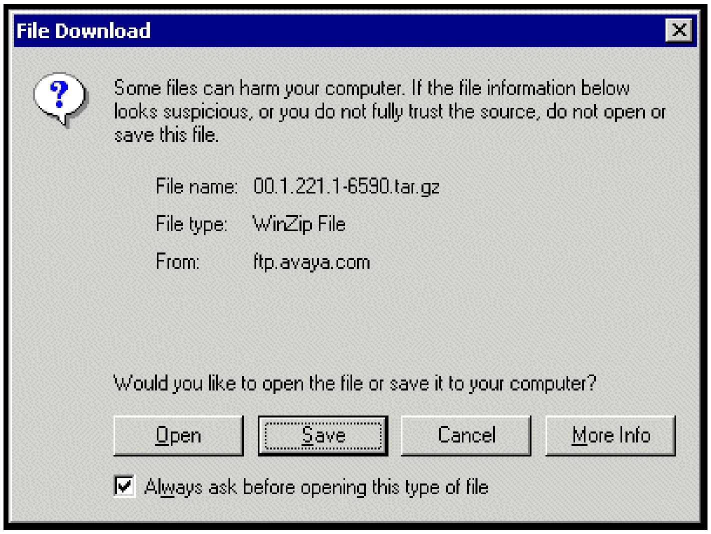
A post-upgrade service pack may be required. If so, download it from http://www.avaya.com/support on the Internet.

Downloading service packs to the laptop

1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access http://www.avaya.com/support on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At the Avaya support site, click **Downloads**.
4. Click **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates**.
5. Scroll down to **Software Update table for Servers running Communication Manager**.
6. Click the link for the appropriate G.A. load.
7. If you are a Business Partner, scroll to the bottom of the page and select **Download Center** to access the password protected Download Center. Otherwise, for Avaya, click **Latest Avaya Communication Manager x.x.x Service Pack** to access the service pack download

   The File Download window appears.

File download window


File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: 00.1.221.1-6590.tar.gz

File type: WinZip File

From: ftp.avaya.com

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

8. Click **Save** and browse to the directory on your laptop in which you want the file saved.

Obtaining service pack and language files for the messaging application, if necessary

If IA770 Intuity Audix messaging application is installed, determine whether a service pack is needed and/or optional languages are used. If so, you will need to obtain the data files.

Checking for IA770 stored messages size

When upgrading Communication Manager to release 5.2 from a previous release, the total volume of messages stored in IA770 must be less than 72 hours due to a change in the voice encoding algorithm from CELP to G.711. Before going to the site, have the customer check the volume of messages stored in IA770. If it is greater than 72 hours, contact your service support center.

To check the IA770 stored messages size

1. In the Maintenance Web Interface, under Miscellaneous, select **Messaging Administration**.

2. Select **System Configuration and Status** > **System Status**.

   Look for “Used Hours of Speech” in the list. If more than 72 hours is reported, the customer must delete some messages before the upgrade.

   or

   Use the CLI command, **`/vs/bin/util/vs_status`**.

Obtaining a messaging service pack file

If a service pack for the messaging application, Communication Manager Messaging, is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an Communication Manager Messaging service pack file

1. On the Avaya Support Web site, click **Find Documentation and Downloads by Product Name**.
2. Under the letter "C", select **Communication Manager Messaging**.
3. Click **Downloads**.

   To download the IA770 patch software:
4. Click **Communication Manager Messaging Application Patches**.
5. Click the service pack file name for this release.

   For example, **C6072rf+b.rpm**.
6. Click **Save** and browse to the location on your laptop where you want to save the file.

   Note:

   The Communication Manager Messaging patch documentation is co-located with the patch software.

Obtaining optional language files

Optional languages are any language other than English (***us-eng*** or ***us-tdd)***. If optional languages are used with this Communication Manager Messaging, you must download the appropriate language files from a language CD after the upgrade. The customer should have the language CD(s) at the site. If not, you need to obtain the appropriate language CD(s) and take them to the site.

Completing the RFA process (obtaining license and authentication files)

Every S8300 Server and local survivable processor (LSP) requires a current and correct version of a Communication Manager license file in order to provide the expected call-processing service. If you are enabling SIP Enablement Services (SES), the S8300 Server also requires an SES license file.

The Communication Manager license file specifies the features and services that are available on the S8300 Server, such as the number of ports purchased. The license file contains a software version number, hardware serial number, expiration date, and feature mask. The license file is reinstalled to add or remove call-processing features. New license files may be required when upgrade software is installed.

The Avaya authentication file contains the logins and passwords to access the S8300 Server, Communication Manager, and SES. This file is updated regularly by Avaya services personnel, if the customer has a maintenance contract. All access from any login is blocked unless a valid authentication file is present on the S8300 Server.

A new license file and the Avaya authentication file may be installed independently of each other or any other server upgrades.

License file and Communication Manager versions for an LSP

The license file for a S8300 configured as a Local Survivable Processor must have a feature set that is equal to or greater than that of the S8300 Server that acts as primary controller (an S8300, S8400, S8500-Series, or S8700-Series Server). This is necessary so that if control passes to the LSP, it can support the same level of call processing as that of the primary controller.

Additionally, the LSP must have a version of Communication Manager that is the same as, or later than, that of the primary controller.

Note:

The license file requirements of the LSP should be identified in your planning documentation.If you are upgrading an LSP, you do *not* install a SES license.

For information on how to acquire an RFA license file, see *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149.

For information on how to acquire an authentication file, see *Authentication File System User Guide*, 03-601703.

Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary

This step is necessary only if the configuration of the customer's INADS alarming modem has changed.

Note:

> ART is available only to Avaya associates. **Business Partners** should call 800-295-0099.

The ART tool is a software tool that generates an IP address for a customer's INADS alarming modem. This IP address is required for configuring the S8300's modem for alarming.

Note:

> You must generate a license and authentication file before you use the ART tool. Also, the ART process is available *only* to Avaya personnel. You need an ART login ID and password, which you can set up at the ART web site. Non-Avaya personnel must contact their service support or customer care center for INADS addresses, if required.

To run the ART

1. Access the ART web site on your laptop at http://ssdp.dr.avaya.com/vtac/jsp/portal.jsp.
2. Use Avaya SSO credentials to log in to the ART Web site.
3. Click **Administer a Communication Manager (CM) product**.
   a. Select **Install Script Administration** as the session type.
   b. Select **S8300 Sever** as the product type.
   c. Click **Start CM Product Administration**.

   A script file is created and downloaded or emailed to you.
4. You can use the installation script to set up an IP address and other alarming parameters automatically.

Obtaining the static *craft* password (Avaya technicians only)

After installing new software and a new Authentication file, you will need to use a static craft password to access the customer's system. This static password will enable you to log in to the S8300 with a direct connection to the Services port without the ASG challenge/response. To obtain the static password, call the ASG Conversant number, 800-248-1234 or 720-444-5557 and follow the prompts to get the password. In addition to your credentials, you will need to enter the customer's Product ID or the FL or IL number.

Business Partners must use the *dadmin* password. Call 877-295-0099 for more information.

On-site preparation for the upgrade

Perform the following tasks before starting the software upgrade on the S8300.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See Laptop configuration for direct connection to the services port on page 31.

You will use telnet, SSH, and the Maintenance Web Interface to perform the procedures. See the following:

- Accessing the server’s command line interface with SSH on page 44
- Logging in to the S8300 Server from your laptop using Telnet on page 45

Logging in to the S8300 Web Interface from your laptop on page 46

Ensuring a super-user login exists

A super-user login must be administered prior to upgrading the S8300 Server. If, for some reason, the server web pages timeout before the authentication file is installed, you must use the super-user login to continue the installation. The project manager, remote services, or the customer should check to verify that one exists. If a super-user login must be added, you must log in as dadmin or a higher level of login. For pre-4.0 releases, you cannot add the login by logging in as craft.

Note:

The passwords you administer for Communication Manager also apply to SES, if SES is enabled.

Checking a pre-4.0 release

To ensure that a super-user login exists in Communication Manager prior to Release 4.0:

1. Log in with **`telnet`** or **`ssh`**.

2. At the SAT command line, enter **list logins**.

   The Logins screen appears.

```
list logins

                                  LOGINS
Login    Service         Status      Pwd. Aging  ASG Blk Expiration  No. of Sess.
         Level                       Cycle (Days)        Date        Sess.  Used

init     init            active                   y  n     /  /
inads    inads           inactive                 y  n     /  /
dadmin   dadmin          inactive                 n  n     /  /
craft    craft           inactive                 y  n     /  /
acpsnmp  non-super-user void                      n  n     /  /
```

3. In the Service Level column, look for a login that has either the `dadmin` or `super-user` level.
4. If a super-user login does not exist, create one. See Creating a super-user login, if one does not exist (releases earlier than Release 4.0) on page 302.

Checking a 4.0 or later release

To ensure that a super-user login exists in Communication Manager in Release 4.0 or higher:

1. Log in with **ssh**.
2. At the Linux command line, type **cat /etc/passwd |grep 555**.

   The following list of super-user logins appears:

```
init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1001:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash
```

3. Look for any logins other than the init, inads, and craft logins.

   If no additional super-user logins exist, you must create one. See Creating a super-user login, if necessary (release 4.0 or 4.0.x only) on page 303, or

   See,Creating a super-user login, if necessary (release 4.1 and later) on page 306.

Creating a super-user login, if one does not exist (releases earlier than Release 4.0)

If a super-user login does not exist, one must be added before you can complete the upgrade. The customer or remote services should complete the following task.

Perform the following procedure only if you are upgrading from a software release *earlier* than Release 4.0.

Note:

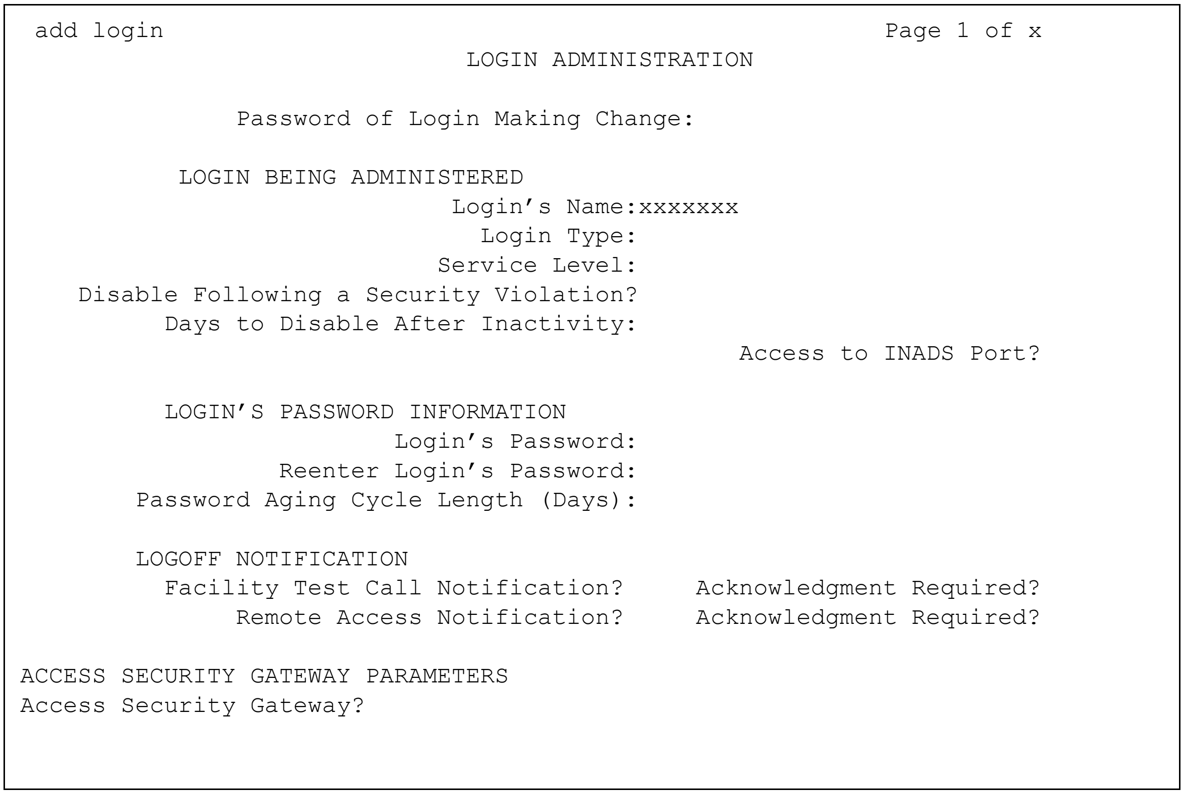
Adding a super-user login with the SAT command line requires a dadmin, init, or inads login.

Note:

If you are upgrading an S8300 LSP, create the super-user login on the primary Controller. Then, on the primary controller SAT, run the **`save translation lsp`** command. If **`save translation lsp`** is not a valid command, run **`save translation`**.

1. At the SAT command line, enter **`add login`**.

   The Login Administration screen appears.



```
 add login                                                   Page 1 of x
                               LOGIN ADMINISTRATION

               Password of Login Making Change:

           LOGIN BEING ADMINISTERED
                              Login’s Name:xxxxxxx
                                Login Type:
                             Service Level:
    Disable Following a Security Violation?
          Days to Disable After Inactivity:
                                                  Access to INADS Port?

          LOGIN’S PASSWORD INFORMATION
                          Login’s Password:
                  Reenter Login’s Password:
        Password Aging Cycle Length (Days):

        LOGOFF NOTIFICATION
          Facility Test Call Notification?     Acknowledgment Required?
               Remote Access Notification?     Acknowledgment Required?

ACCESS SECURITY GATEWAY PARAMETERS
Access Security Gateway?
```

2. In the **Password of Login Making Change** field, type your password.

3. In the **Login's Name** field, type a login name agreed upon with the customer. Alternatively, a Business Partner may add the dadmin login.
4. In the **Login Type** field, type **customer**.
5. In the **Service Level** field, type **super-user**.
6. In the **Days to Disable After Inactivity** field, type **90**.
7. In the **Login's Password** field, type a password.
8. In the **Reenter Login's Password** field, type the password again.
9. In the **Password Aging Cycle Length** field, type **90**, and press **Enter**.
10. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.
    a. Log in with **`telnet`** or **`ssh`**, open a SAT window.
    b. At the primary controller SAT, run the **`save translation lsp`** command. If **`save translaton lsp`** is not a valid command, run **`save translation.`**

Creating a super-user login, if necessary (release 4.0 or 4.0.x only)

Perform this task if the server is running Communication Manager release is 4.0 or 4.0.x.

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages.

Note:

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

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, on the primary controller SAT, run the **`save translation lsp`** command.

To create a login:

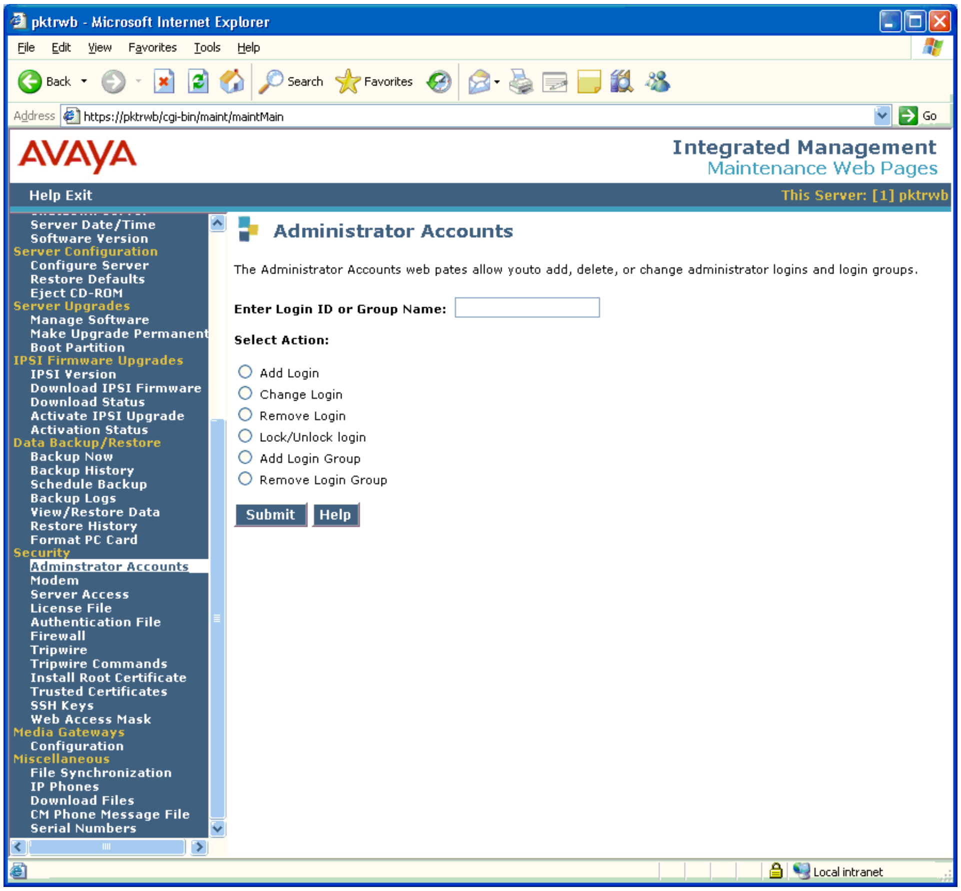
1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

   Note:

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

2. Under **Security**, select **Administrator Accounts**.

   The **Administrator Accounts** screen appears.



Administrator Accounts

The Administrator Accounts web pates allow youto add, delete, or change administrator logins and login groups.

Enter Login ID or Group Name:

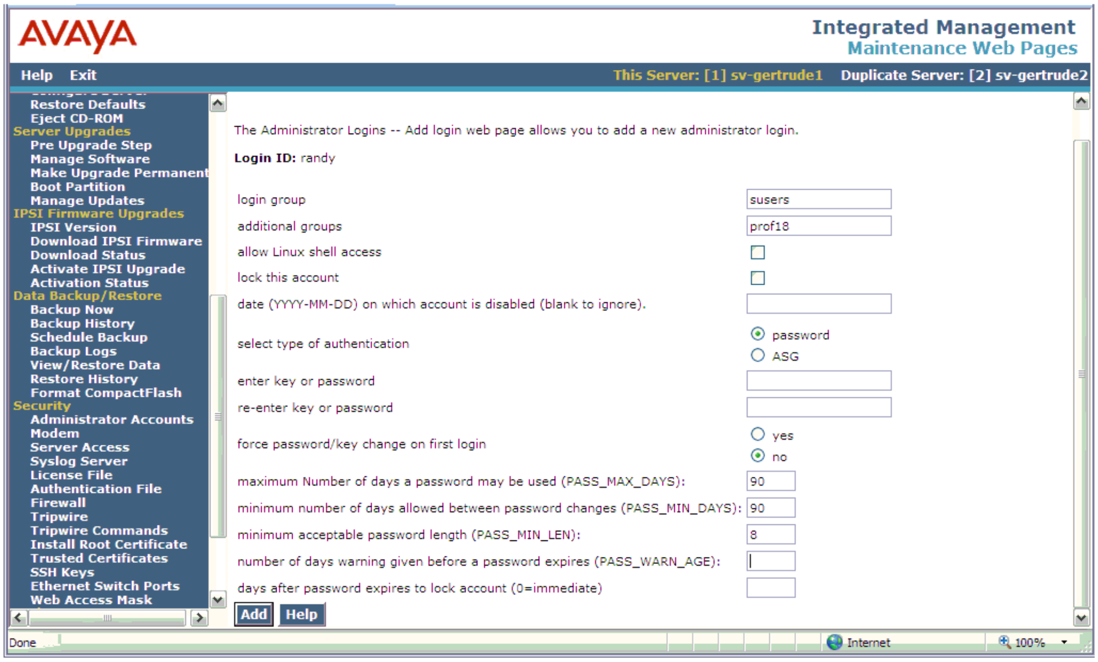
Select Action:

○ Add Login
○ Change Login
○ Remove Login
○ Lock/Unlock login
○ Add Login Group
○ Remove Login Group

3. Type the login name in the **Enter Login ID or Group Name** field.

4. Select **Add Login**, and click **Submit**.

   The Administrator Logins -- Add Login screen appears.



The Administrator Logins -- Add login web page allows you to add a new administrator login.

Login ID: randy

login group	susers
additional groups	prof18
allow Linux shell access	□
lock this account	□
date (YYYY-MM-DD) on which account is disabled (blank to ignore).	
select type of authentication	● password ○ ASG
enter key or password	
re-enter key or password	
force password/key change on first login	○ yes ● no
maximum Number of days a password may be used (PASS_MAX_DAYS):	90
minimum number of days allowed between password changes (PASS_MIN_DAYS):	90
minimum acceptable password length (PASS_MIN_LEN):	8
number of days warning given before a password expires (PASS_WARN_AGE):	
days after password expires to lock account (0=immediate)	

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer super-user.
7. Select the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.
10. Complete the following fields:
    - enter a challenge key or password
    - re-enter challenge key or password
    - force password/key change on first login

    Note:

    Do not lock the account or set the password to be disabled.
11. Leave the defaults in the remaining fields.
12. Click **Add**.

    A message appears that the login has been added successfully.
13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

a. Log in with `telnet` or `ssh`, open a SAT window.

b. At the primary controller SATL, run the `save translation lsp` command.

Creating a super-user login, if necessary (release 4.1 and later)

You must add a super-user account, also known as priveledged user account before you use Avaya Installation Wizard to configure the server and install the Avaya authentication file.

Note:

The passwords you administer for Communication Manager also apply to SES, if SES is optioned.

Note:

A craft level login can create a super-user login from Communication Manager release 4.0 or later.

To create a login:

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

   Note:

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

2. On the Communication Manager System Management Interface Web page, click **Server (Maintenance)** under the **Administration** menu.
3. Select **Security** > **Administrator Accounts**.

   The **Administrator Accounts** screen appears.
4. Select **Add Login**.
5. Select **Privileged Administrator** and click **Submit**.

   The **Administrator Logins -- Add Login: Privileged Administrator** screen appears.
6. Type a login name for the account in the **Login name** field.
7. Verify the following:
   - **susers** appears in the **Primary group** field.
   - **prof18** appears in the **Additional groups (profile)** field. *prof18* is the code for the customer super-user.
   - **/bin/bash** appears in the **Linux shell** field.
   - **/var/home/*login name*** appears in the **Home directory** field, where ***login name*** is the name you entered in step 6.

8. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
9. For the **Select type of authentication** option, select **password**.

   Note:

   Do not lock the account or set the password to be disabled.
10. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
11. In the section **Force password/key change on next login** select **no**.
12. Click **Submit**.

    The system informs you the login is added successfully.

Copying a pre-upgrade service pack file to the S8300 Server

To copy a pre-upgrade service pack file to the S8300 Server:

1. On the Maintenance Web Interface, under Miscellaneous, click `Download Files`.
2. Select the download method, **Files to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the checkbox, **Install this file on the local server**.
3. Browse to the directory on the software CD (or laptop) that contains the pre-upgrade service pack file.
4. Select the pre-upgrade service pack file and click **Download**.

Removing the administration for the IA770 integration if CWY1 board is used

Note:

If the S8300 is configured as an LSP, skip to Backing up data on the S8300 Server on page 316.

⚠ **CAUTION:**

Communication Manager Release 5.2 does not support the CWY1 method of integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current switch integration administration now. You must administer the integration for H.323 after the upgrade.

For instructions on removal of existing CWY1 administration, see *Administering Media Servers to Work with IA770*.

Note:

For Releases 2.0 and 2.1 of Communication Manager that use IA770, you *cannot* remove messaging from the Media Gateway screen in the SAT interface *before* the upgrade. Therefore, you must remove messaging from Slot V8 of the Media Gateway screen after the upgrade, then administer the H.323 integration.

Completing pre-upgrade tasks — if the target S8300 is the primary controller

If the S8300 is configured as an LSP, skip to Backing up data on the S8300 Server on page 316.

⚠ **CAUTION:**

If you are upgrading an S8300 primary controller that has LSPs registered to it, the LSPs must be upgraded before the primary controller. You can use the SAT command **`display lsp`** or **`list survivable-processor`** to determine if there are LSPs registered to the S8300.

Perform the following procedures if you are upgrading an S8300 that is configured as a primary controller:

- To display IA770 alarms, if IA770 is enabled
- To clear alarms
- To check link status
- To record all busyouts
- To disable scheduled maintenance
- To check for translation corruption
- To save translations
- To disable alarm origination

To display IA770 alarms, if IA770 is enabled

1. In the Maintenance Web Interface, click **Messaging Administration**.
2. On the Messaging Administration menu, under Logs, click **Alarm**.
3. On the Alarm Log screen, type today's date. Leave the defaults in all other fields.
4. Click **Display**.
5. Resolve any alarms that are listed.

To clear alarms

1. In the Maintenance Web Interface under Alarms, click **Current Alarms**.
2. If no alarms are listed, skip the next two steps.
3. If alarms are listed, click **Clear All**.
4. Resolve any remaining major alarms through the Communication Manager SAT.

To check link status

1. Open a SAT session.
2. Enter **`display communication-interface links`**.
3. Note all administered links.
4. Enter **`status link`** ***`number`*** for each administered link.
5. Enter **`list signaling group`**.
6. Note the signaling groups listed by number.
7. For each of the signaling groups listed, enter **`status signaling group`** ***`number`***.
8. Make a note (write down) of any links that are down.

To record all busyouts

1. At the SAT prompt, type **display errors**, and press **Enter**.
2. Look for type 18 errors and record (write down) any trunks that are busied out. You must return them to their busy-out state after the upgrade.

To disable scheduled maintenance

Scheduled daily maintenance must not interfere with the upgrade.

1. At the SAT prompt, type **`change system-parameters maintenance`** and press **Enter**.
2. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

   or,

   If scheduled maintenance is not in progress, set the **Start Time** field to a time after the upgrade will be completed.

   For example, if you start the upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to 21:30.

To check for translation corruption

1. At the SAT prompt, type **`newterm`** and press **Enter**.

2. Enter your terminal type, and press **Enter**.

   If the following message appears,

   ```
   Warning: Translation corruption found
   ```

   follow the normal escalation procedure for translation corruption before continuing the upgrade.

To save translations

1. At the SAT prompt, type **`save translation`** and press **Enter**.
2. Under **Command Completion Status** you should see the message, `Success`.

To disable alarm origination

If alarm origination is enabled during the upgrade, unnecessary alarms will be sent to the Operations Support System (OSS) destination number(s). Even if you selected **Suppress Alarm Origination** when you logged in, alarm origination will be automatically re-enabled when the system reboots after the software upgrade. Use this procedure to prevent alarm origination from being re-enabled after reboot.

CAUTION:

If you do not disable alarm origination, the system can generate alarms during the upgrade, resulting in unnecessary trouble tickets.

1. Logoff the SAT session.
2. At the command prompt, type **`almenable -d n -s n`**, where

   `-d n` sets the dialout option to **`neither`** (number)

   `-s n` disables SNMP alarm origination

   Note:

   Be sure to reset alarm origination after the upgrade.
3. Type **`almenable`** (without any options) to verify the alarm origination status.

   You should see:

   ```
   incoming: enable

   Dial Out Alarm Origination: neither

   SNMP Alarm Origination: n
   ```

Saving a copy of the 4600-series telephone configuration file, if any

Note:

Skip this procedure if the release is 3.1.3 or later.

If the S8300 is used to support firmware downloads to IP telephones and the current software load is 2.x (R012x.00.0.219..0) through 3.1.2 (R013x.01.2.632.1), you must perform this procedure.

If the S8300 is used to support firmware downloads to IP telephones and the current software load is 2.x (R012x.00.0.219..0) through 3.1.2 (R013x.01.2.632.1), you must perform this procedure.

⚠ **Important:**

The 46xxsettings.txt file must be saved to the services laptop or to another backup server *before* the S8300 is removed from service.

After the S8300 is upgraded, you must restore the 46xxsettings.txt file and the IP telephone firmware files to the S8300 Server. For more information, see Copying IP Phone firmware to the server, if necessary on page 343.

Use the following steps to copy the 46xxsettings.txt file to the services laptop or backup server:

1. At the server command line interface, type **`cp/tftpboot/46xxsettings.txt /var/home/ftp/pub`**.
2. Use FTP or SFTP to move the 46xxsettings.txt file to the services laptop or backup server.

Getting IA770 data and Stopping IA770 (if IA770 is being used)

Skip to Backing up data on the S8300 Server on page 316 if IA770 is not being used.

If IA770 is being used, you need to collect optional language data (if this had not been done before arriving at the site), leave a test message, and shut down IA770 before backing up the files.

Determining whether optional languages are needed

To determine the system language

⚠ **CAUTION:**

If an announcement package appears on the Web page that follows, that package *must* be present after the upgrade and before you restart messaging. For example, if British English is a package that has been installed, you must back up the package before the upgrade and restore it immediately after the upgrade. If an announcement set present before the upgrade is not present after the upgrade, IA770 cannot be restarted.

1. In the Maintenance Web Interface, under Miscellaneous, select **Messaging Administration**.

   The Messaging Administration Web page appears.

2. Select **Messaging** in the left-hand navigation pane.

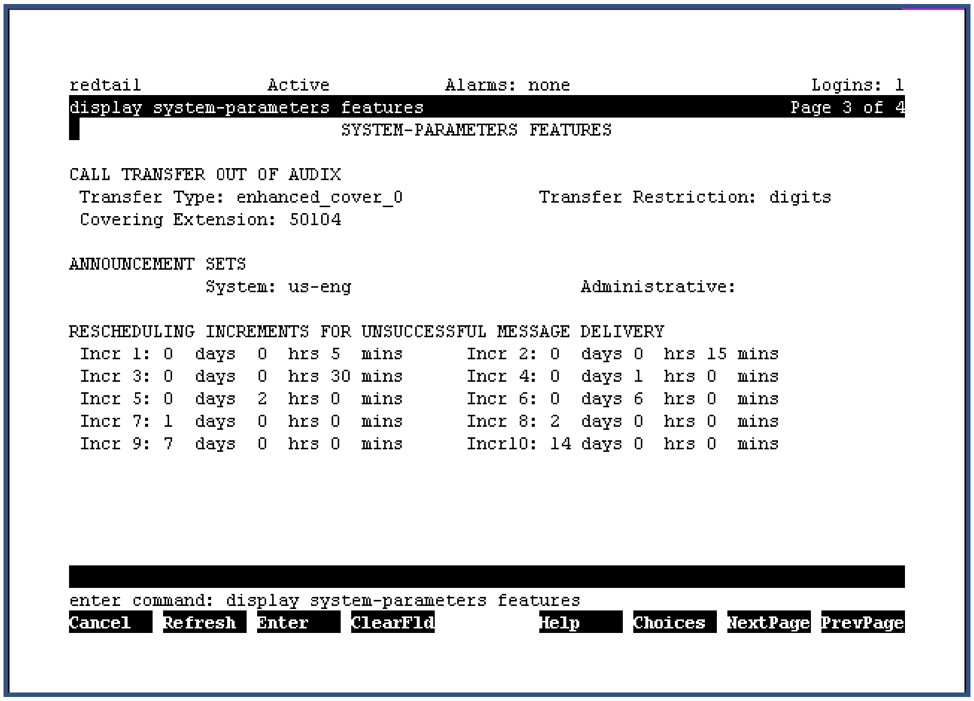
   Security certificates appear.

3. Accept the security certificates.
4. Enter the *craft* password.
5. At the command prompt, enter **display system-parameters features**.

   The **SYSTEM PARAMETERS FEATURES** screen appears.

6. Go to page 3.

System Parameters Features screen, Page 3



```
redtail             Active           Alarms: none                  Logins: 1
display system-parameters features                                Page 3 of 4
                          SYSTEM-PARAMETERS FEATURES

CALL TRANSFER OUT OF AUDIX
 Transfer Type: enhanced_cover_0           Transfer Restriction: digits
 Covering Extension: 50104

ANNOUNCEMENT SETS
             System: us-eng                    Administrative:

RESCHEDULING INCREMENTS FOR UNSUCCESSFUL MESSAGE DELIVERY
 Incr 1: 0  days  0  hrs 5  mins      Incr 2: 0  days 0  hrs 15 mins
 Incr 3: 0  days  0  hrs 30 mins      Incr 4: 0  days 1  hrs 0  mins
 Incr 5: 0  days  2  hrs 0  mins      Incr 6: 0  days 6  hrs 0  mins
 Incr 7: 1  days  0  hrs 0  mins      Incr 8: 2  days 0  hrs 0  mins
 Incr 9: 7  days  0  hrs 0  mins      Incr10: 14 days 0  hrs 0  mins




enter command: display system-parameters features
```

7. Under **Announcement Sets**, note the main system language listed after **System:** In this example, the main system language is English (**us-eng**). If any language files other than these two are listed, you will need to download the additional language files from a language CD after the upgrade or backup and restore the announcement files.

   Note:

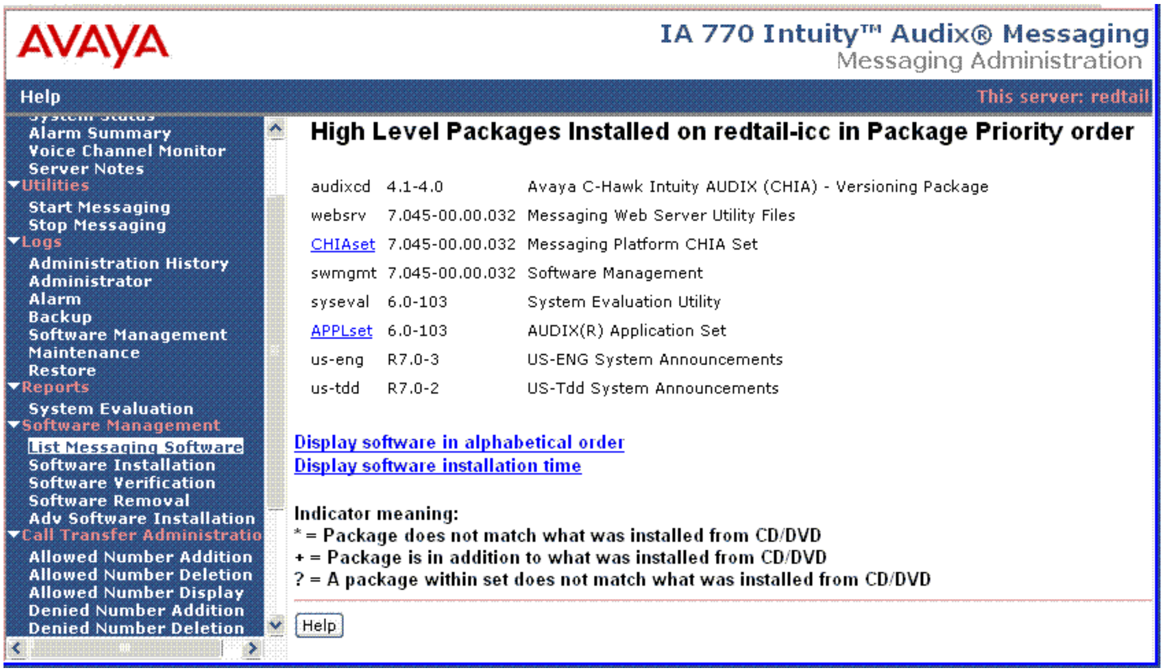
   Starting with release 2.1, only English language files (**us-eng** and **us-tdd**) are included with the Communication Manager software. Before release 2.1, Latin American Spanish and Canadian French (**lat-span** and **french-c**) were also included.

To determine other languages

1. In the Maintenance Web Interface, under Miscellaneous, select **Messaging Administration**.
2. Under **Software Management**, select **List Messaging Software**.

   The **List Messaging Software** screen appears.

List Messaging Software screen



High Level Packages Installed on redtail-icc in Package Priority order

audixcd	4.1-4.0	Avaya C-Hawk Intuity AUDIX (CHIA) - Versioning Package
websrv	7.045-00.00.032	Messaging Web Server Utility Files
CHIAset	7.045-00.00.032	Messaging Platform CHIA Set
swmgmt	7.045-00.00.032	Software Management
syseval	6.0-103	System Evaluation Utility
APPLset	6.0-103	AUDIX(R) Application Set
us-eng	R7.0-3	US-ENG System Announcements
us-tdd	R7.0-2	US-Tdd System Announcements

Display software in alphabetical order

Display software installation time

Indicator meaning:
* = Package does not match what was installed from CD/DVD
+ = Package is in addition to what was installed from CD/DVD
? = A package within set does not match what was installed from CD/DVD

Help

3. Note the **System Announcement** language files listed. In this example, **us-eng** and **us-tdd** are listed. If any language files other than these two are listed, you will need to download the additional language files from a language CD after the upgrade or backup and restore the announcement files.

Downloading optional language files, if needed

Skip to To shut down IA770 with the command line interface on page 315 if optional language files are not needed. If the optional language files are needed, copy the files from the language CD to
/var/home/ftp/pub.

To download optional language files

1. Insert the optional language CD in your laptop's CD-ROM drive.
2. In the Maintenance Web Interface, under Miscellaneous, select **Download Files**.
3. Select the **Files to download from the machine I'm using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click the **Download** button.

   When the transfer is complete, the following message appears:

   ```
   Files have been successfully downloaded to the server
   ```
6. If more than four optional language files need to be downloaded, repeat this procedure.

Copies of the optional language files are now in the **/var/home/ftp/pub** directory and will be automatically installed during the upgrade process.

Creating an test message for the upgrade

To test IA770 after the upgrade

1. Write down the number of a test voice mailbox, or create one if none exists.
2. Write down the number of the IA770 hunt group.
3. Leave a message on the test mailbox that will be retrieved after the upgrade.

Shutting down IA770

To shut down IA770 with the command line interface

1. Type `telnet 192.11.13.6` and press **Enter**.
2. Log in as *craft* or *dadmin*.
3. Type `stop -s Audix` and press **Enter** to shut down AUDIX. Note that the "A" in Audix must be capitalized.

   The shutdown will take a few minutes.

4. Type **watch /VM/bin/ss** and press **Enter** to monitor the shutdown.

   The watch command will automatically refresh every few seconds. When the shutdown is complete, you will see only the voicemail and audit processes. For example:

   voicemail:(10)

   audit http:(9)

   Press **Ctrl+C** to break out of the **watch** command.

5. Type **/vs/bin/util/vs_status** and press **Enter** to verify that AUDIX is shut down.

   When AUDIX is shut down, the following message appears:

   ```
   voice system is down
   ```

   ⚠ **Important:**
   After upgrading an S8300, you must upgrade the media gateway and media module firmware before restarting IA770.

To shut down IA770 with the Maintenance Web pages

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. Under **Utilities**, select **Stop Messaging**.

   The **Stop Messaging Software** Web page is displayed.

3. Select the **Stop** button.

   The shutdown of the messaging server will begin when all users have logged off from IA770 or after three minutes have passed, whichever event comes first. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

   ⚠ **Important:**
   After upgrading an S8300, you must upgrade the media gateway and media module firmware before restarting IA770.

Backing up data on the S8300 Server

Before upgrading the S8300, back up the system data in case you need to back out of the upgrade.

Depending on the existing software release you can back up the S8300-Series Server data by:

- Backing up the system to compact flash media on page 317
- Backing up the system over the customer's LAN on page 318

Backing up the system to compact flash media

S8300C Server allows back up using a compact flash card.

To back up the system to compact flash media

1. Plug the cable to the compact flash drive into a USB port on the S8300C Server.
2. Insert a 128-Mb compact flash media into the card reader or writer.
3. On the Maintenance Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.
4. In the Data Sets section select all of the following data sets:
   - If the S8300B, S8300C Server is ***not*** an LSP, select **Avaya Call Processing** (**ACP**) **Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - **SES Files** (seen as an option if SES is enabled)
   - If Communication Manager Messaging is installed on an S8300B or S8300C Server, select **Audix**. Also select **Translations, Names and Messages**.

   Note:

   Depending on the customer's Communication Manager Messaging configuration, the back up size of the Communication Manager Messaging data set (**Translations, Names and Messages)** can be larger than the size of the compact flash drive (maximum size of the compact flash drive is 128 MB).
5. Select the Backup Method:
   - Local PC Card

   Tip:

   Backing up to the USB Compact Flash saves time when you are restore data to the migrated server.
6. Optionally, select **Format Compact Flash** to format a new card.

   Note:

   The compact flash card needs to be formatted only before the first use.
7. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

Backing up the system over the customer's LAN

You can back up to an FTP, SFTP, or SCP Server on the customer's network. To back up to an server over the customer's LAN, you need the IP address, directory path, user credentials of the server.

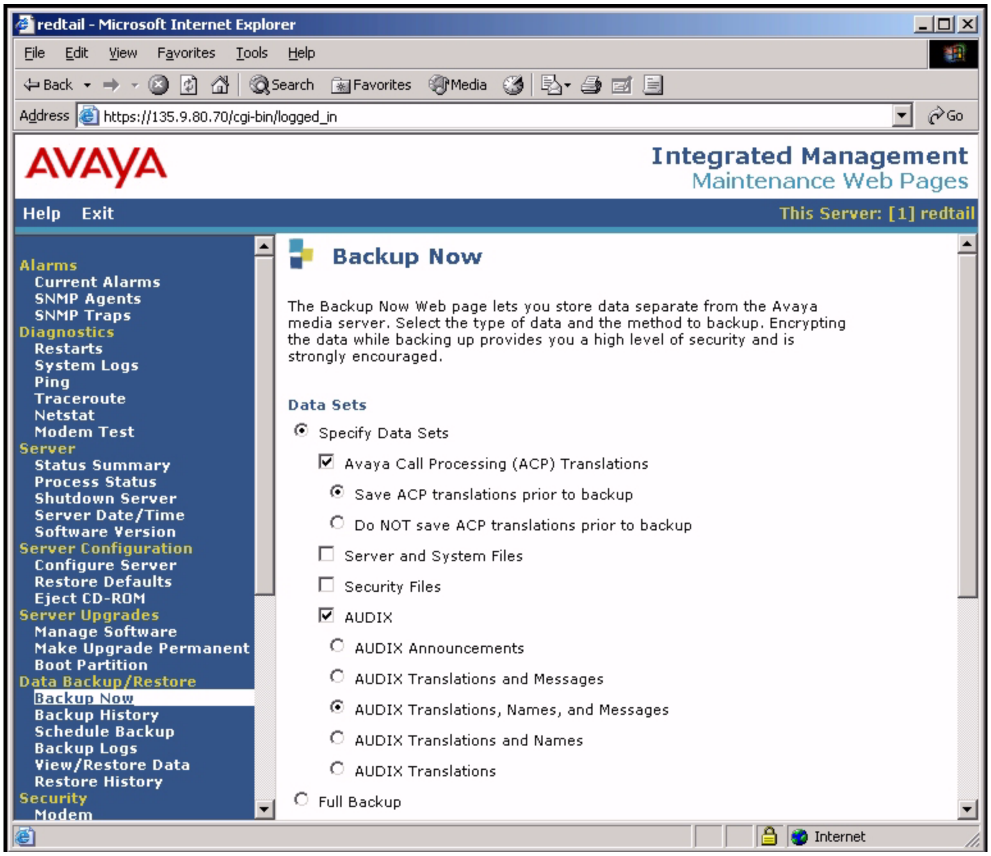
Check with your project manager or the customer for this information.

To back up S8300 recovery system data:

1. Under **Data Backup/Restore**, click **Backup Now**.

   The **Backup Now** screen appears.

Backup Now screen (Part One)



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

● Specify 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

☑ AUDIX

○ AUDIX Announcements

○ AUDIX Translations and Messages

● AUDIX Translations, Names, and Messages

○ AUDIX Translations and Names

○ AUDIX Translations

○ Full Backup

2. Select **Full Backup**, if available with the existing release, or select all data sets:

   - **Avaya Call Processing (ACP) Translations**; select **Save ACP translations prior to backup**

   Note:

   > Select ACP translations only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

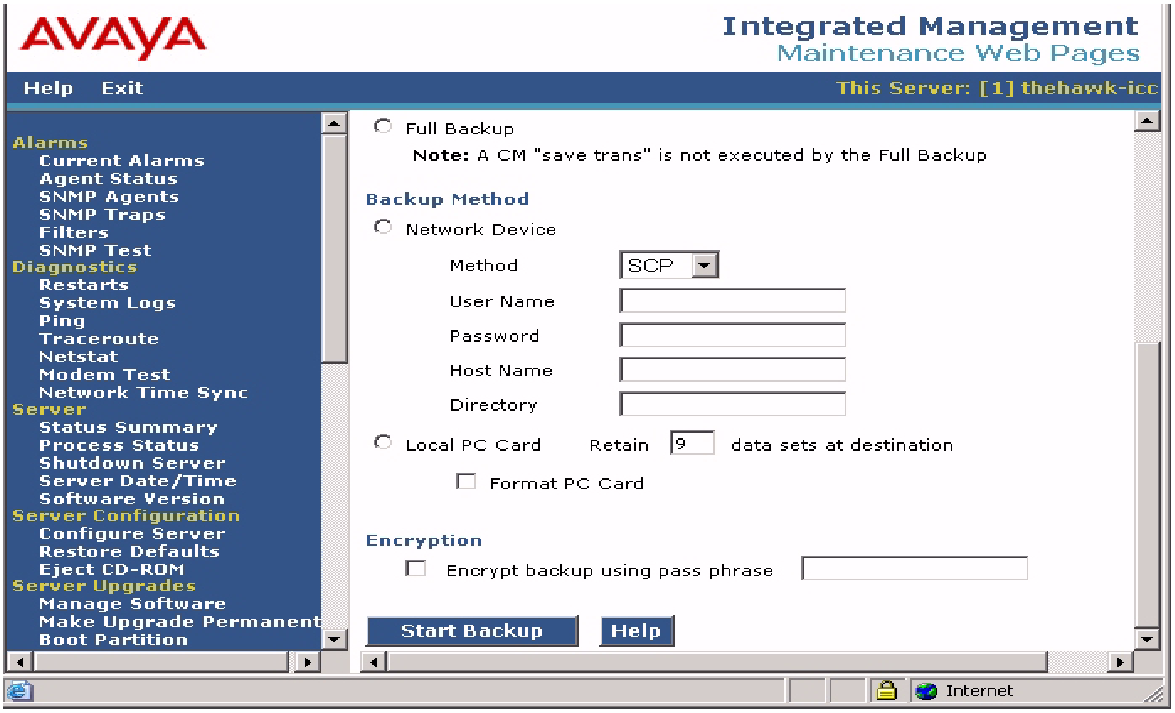
- **Server and System Files**
- **Security Files**
- **SES Files** (seen as an option if SES is enabled)**)**

3. If the AUDIX options are available, select AUDIX and select AUDIX Translations, Names, Messages, and Announcements.

CAUTION:

Selecting the **Full Backup** radio button does NOT include AUDIX files. You must backup the IA770 INTUITY AUDIX data after you do the full backup.

Backup Now screen (Part Two)



○ Full Backup

Note: A CM "save trans" is not executed by the Full Backup

Backup Method

○ Network Device

Method: SCP

User Name:

Password:

Host Name:

Directory:

○ Local PC Card   Retain 9 data sets at destination

□ Format PC Card

Encryption

□ Encrypt backup using pass phrase

Start Backup   Help

4. Select **Network Device**, select the method from the **Method** drop down menu, and fill in the appropriate fields with information provided by the customer.

5. Click **Start Backup** to back up the files.

Note:

The backup and restore processes use the ping service to check connectivity to the backup server. If a backup or restore operation fails, ensure that the ping service is enabled:
i. In the Maintenance Web Interface, under **Security**, select **Firewall**.
ii. In the **Service** column, find **ping**.

The checkboxes for both **Input to Server** and **Output from Server** should be checked.

6. To check the status of the backup:
   a. Under **Data Backup/Restore**, click **Backup History**.
   b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

   When the backup is finished, the **Backup History Results** screen displays the following message:

   ```
   The final status for your backup job is shown below
   ```

   For each backup set, the following message is displayed if the set was backed up successfully:

   ```
   BACKUP SUCCESSFUL
   ```

7. If the AUDIX options are available, repeat Steps 3–6 for AUDIX Announcements.

Copying and installing the service pack files to the S8300 Server (starting from R2.x or from R4.x only)

Note:

Do not perform this task if you are upgrading an R3.x release to R5.2.

A pre-upgrade service pack is required to modify the server upgrade tools, including the web Interface and upgrade scripts, which will enable the upgrade to Communication Manager 5.2 to complete successfully.

To install the pre-upgrade service pack on R2.x systems

Note:

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

The following steps activate the service pack:

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **telnet 192.11.13.6** and press **Enter.**
3. Log in as either *craft* or *dadmin*.
4. Type `update_unpack` and press **Enter**.
5. Select the number corresponding to the service pack file. (For example, `00.0.339.4-xxxx.tar.gz`.) Press **Enter**.
6. Type `update_show` and press **Enter** to list Communication Manager files to verify that the new service pack file was unpacked.

7. Type **`update_activate`** ***`update`***, where ***`update`*** is the release or issue number of the latest service pack file. (For example, **`00.0.339.4-xxxx`**. Do *not* use the .tar.gz extension at the end of the file name.) Press **Enter**.

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

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

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

   The media server displays a message that the service pack was applied.

8. Enter **y** in response to the question, `Commit this software?`

9. Enter **`update_show`** again and press **Enter** to list Communication Manager files to verify the service pack file was activated.

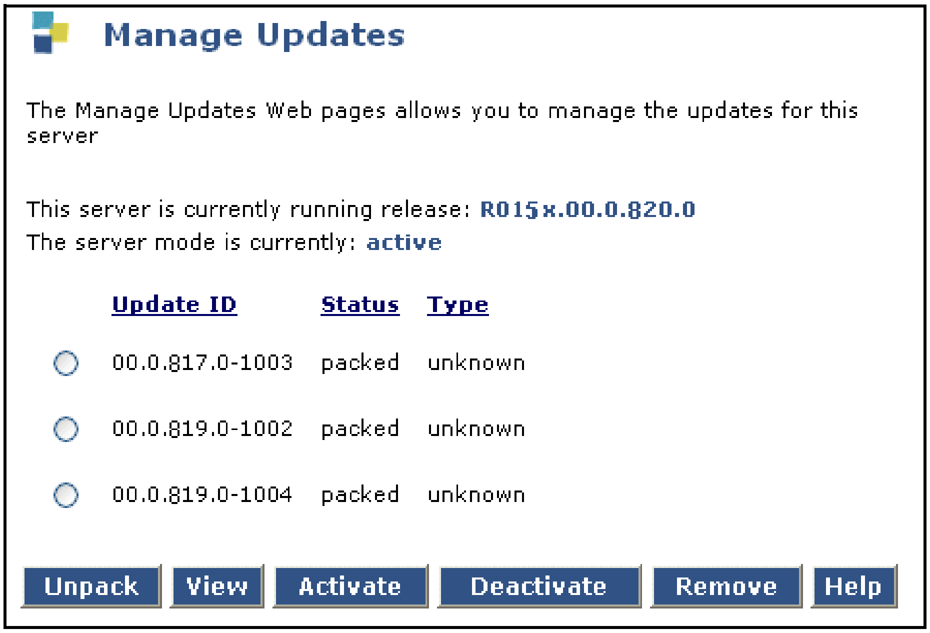
10. Click **Refresh** on the web browser to see the **Manage Software** link on the Maintenance Web Interface.

To install the pre-upgrade service pack on R4.0 Servers

1. Under Server Upgrades, select **Manage Updates**.

   The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allows you to manage the updates for this server

This server is currently running release: R015x.00.0.820.0

The server mode is currently: active

	Update ID	Status	Type
○	00.0.817.0-1003	packed	unknown
○	00.0.819.0-1002	packed	unknown
○	00.0.819.0-1004	packed	unknown

2. If an update file you want to activate shows **packed** in the **Status** column, select update ID and click **Unpack**.

   The window shows the status of the unpacking.

3. Wait until the system displays the message, `... unpacked successfully`, and click **Continue**.

   The system displays the **Manage Updates** screen.

4. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

   The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

5. Click **Yes**.

   Wait until the system displays the **Continue** button.

6. Click **Continue**.

Copying Files to the S8300 hard drive

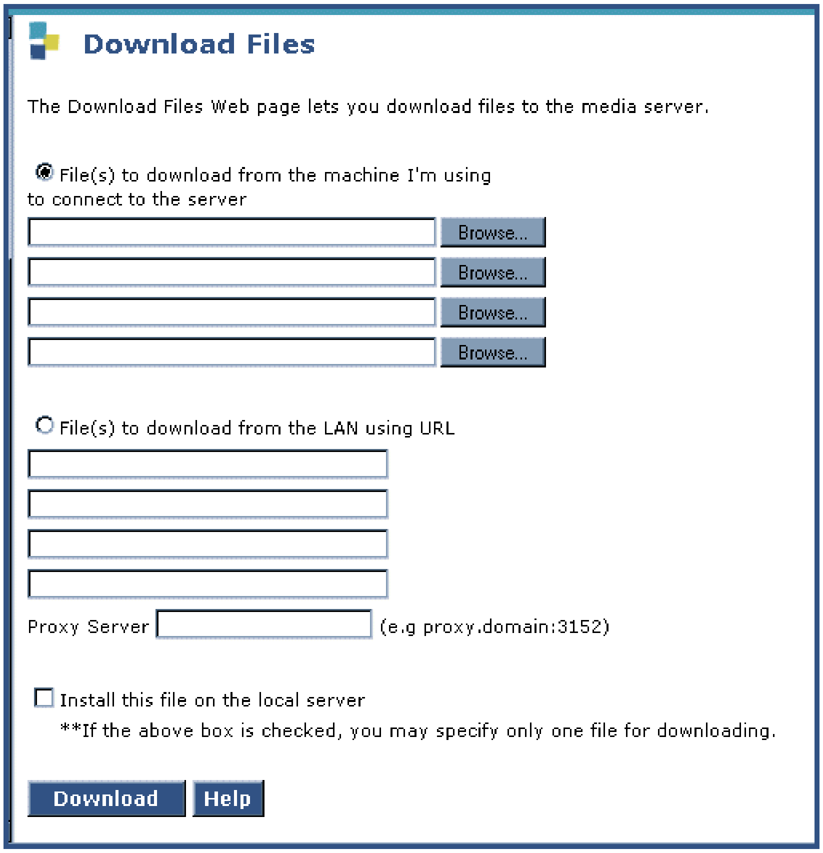
You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Post-upgrade Communication Manager software service pack
- License files (for Communication Manager, and optionally, for SES)
- Avaya authentication file
- New firmware files
- Security updates
- IA770 service packs, RFUs, announcement files, or language sets

To copy files to the S8300 hard drive

1. Under **Miscellaneous** in the Maintenance Web pages, click **Download Files**.

Download Files screen



Download Files

The Download Files Web page lets you download files to the media server.

● File(s) to download from the machine I'm using to connect to the server

○ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

□ Install this file on the local server

**If the above box is checked, you may specify only one file for downloading.

2. Select **Files to download from the machine I'm using to connect to the server** and browse to each file you want to copy to the S8300. Leave the **Install this file on the local server** checkbox ***unchecked.***

   Note:

   To manually FTP files from your laptop to */var/home/ftp/pub*, you must change the directory to *pub* after starting ftp and logging in; that is, type **`cd pub`**.

3. Click **Download** to copy the files to the S8300. The transfer is complete when the following message appears:

```
Files have been successfully downloaded to the server
```

Copying the software and firmware files to the server

Normally, during an upgrade, you will have the Communication Manager Software Distribution CD-ROM that contains the latest software to install, including SIP Enablement Services (SES) and IA770 software. The latest software for the S8300 has a file name that reflects the most recent load of software (*for example only*, 014-01.0.829.1). The latest service pack software for

Communication Manager also reflects the most recent load of software (*for example only*, 05.0-01.0.829.0).

⚠ **CAUTION:**

> When you are upgrading the S8300 Server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the S8300 Server to a release that is not supported as an upgrade path, you might corrupt the translations.
>
> Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.
>
> To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access http://support.avaya.com. Select **Downloads** > **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates** > **Latest Communication Manager Software & Firmware Compatibility Matrix**.

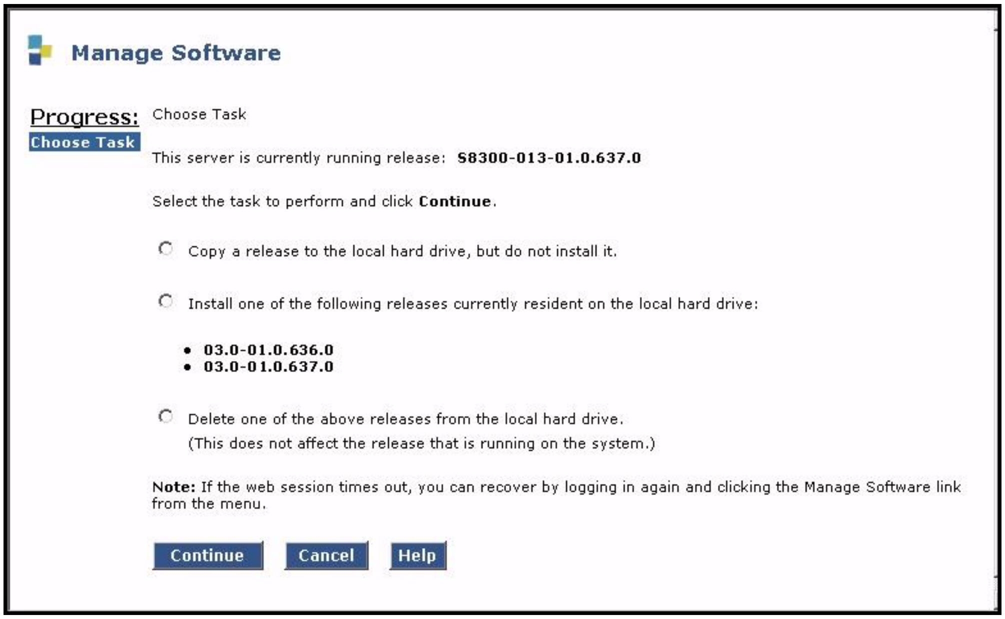
These files also contain the most recent firmware for the media gateway, the various media modules.

To transfer files from the software CD

1. Insert the Communication Manager software distribution CD into the CD-ROM drive.
2. Log in to the S8300 Web interface.
3. Under Server Upgrades, click **Manage Software**.

   The system displays the **Manage Software** screen.

Manage Software screen



Manage Software

Progress: Choose Task

Choose Task

This server is currently running release: **S8300-013-01.0.637.0**

Select the task to perform and click **Continue**.

○ Copy a release to the local hard drive, but do not install it.

○ Install one of the following releases currently resident on the local hard drive:

- **03.0-01.0.636.0**
- **03.0-01.0.637.0**

○ Delete one of the above releases from the local hard drive.
(This does not affect the release that is running on the system.)

Note: If the web session times out, you can recover by logging in again and clicking the Manage Software link from the menu.

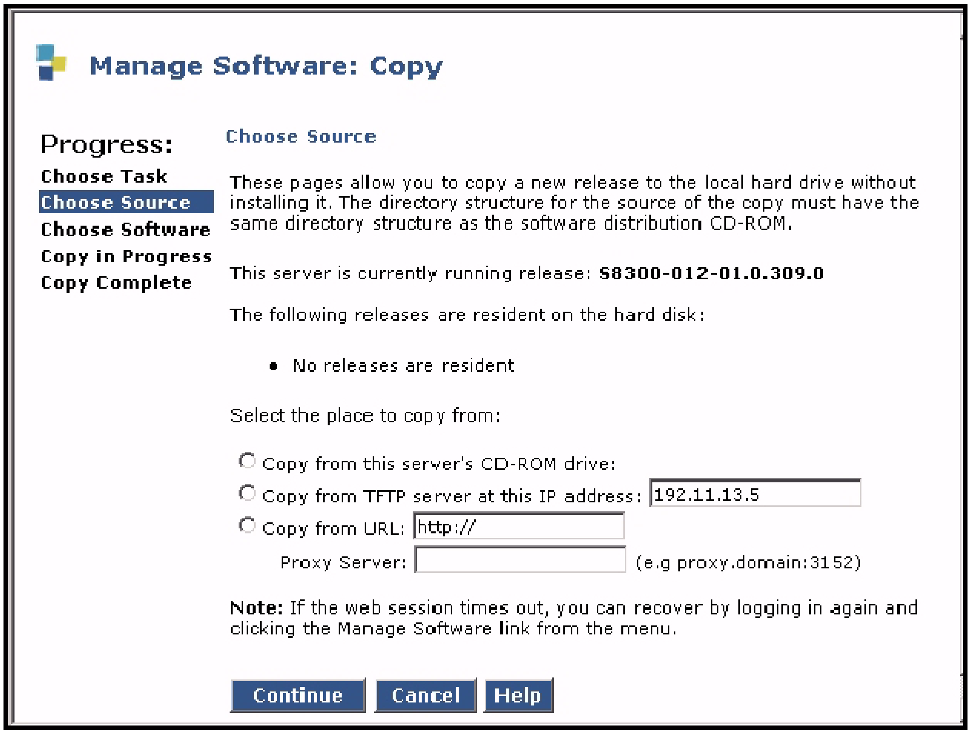
4. Select the radio button **Copy a release to the local hard drive, but do not install it**.

Note:

> The S8300 hard drive can hold up to three releases without having to delete a release before copying a new release from the Communication Manager software distribution CD.

The S8300 displays the **Choose Source** screen, which allows you to copy files from one of several possible sources to the S8300 hard drive.

Choose Source screen



Manage Software: Copy

Choose Source

These pages allow you to copy a new release to the local hard drive without installing it. The directory structure for the source of the copy must have the same directory structure as the software distribution CD-ROM.

This server is currently running release: **S8300-012-01.0.309.0**

The following releases are resident on the hard disk:

- No releases are resident

Select the place to copy from:

○ Copy from this server's CD-ROM drive:

○ Copy from TFTP server at this IP address: 192.11.13.5

○ Copy from URL: http://

Proxy Server: (e.g proxy.domain:3152)

Note: If the web session times out, you can recover by logging in again and clicking the Manage Software link from the menu.

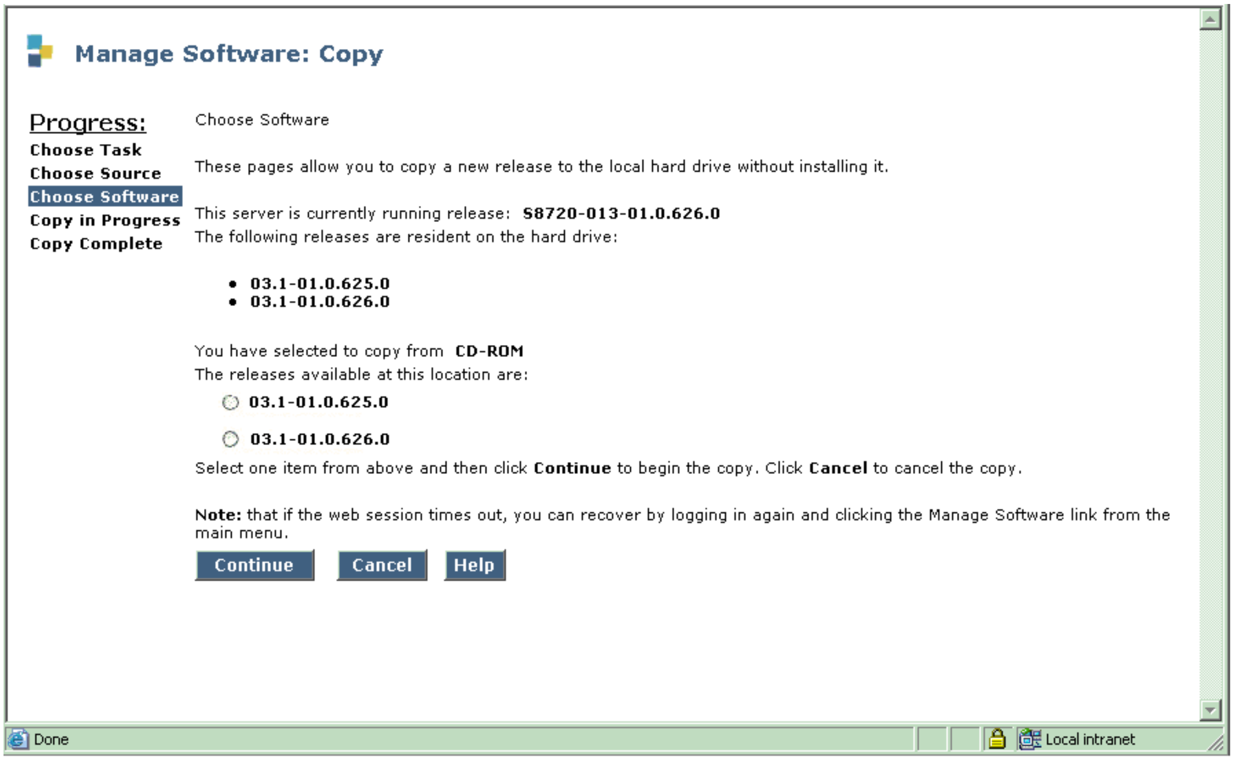
Possible sources include:

- This server’s CD-ROM drive
- TFTP server at IP address shown (default is local laptop at 192.11.13.5)
- URL specified in **Copy from URL:** field

If you select the **Copy from this server’s CD-ROM drive:** radio button, all available CD drives are checked. The first drive found with a valid release is used, in the event multiple CD drives are actually present.

The system displays the **Choose Software** screen.

Choose Software screen



Choose Software

These pages allow you to copy a new release to the local hard drive without installing it.

This server is currently running release: **S8720-013-01.0.626.0**
The following releases are resident on the hard drive:

- **03.1-01.0.625.0**
- **03.1-01.0.626.0**

You have selected to copy from **CD-ROM**
The releases available at this location are:

○ **03.1-01.0.625.0**

○ **03.1-01.0.626.0**

Select one item from above and then click **Continue** to begin the copy. Click **Cancel** to cancel the copy.

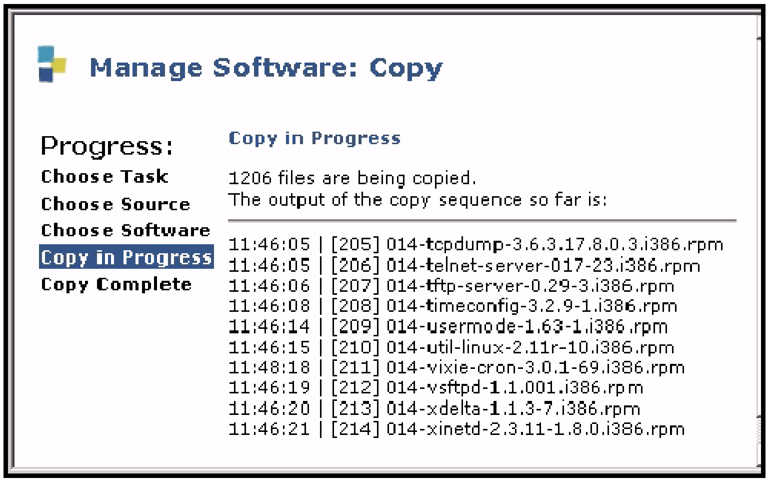
Note: that if the web session times out, you can recover by logging in again and clicking the Manage Software link from the main menu.

The screen appears with no radio button selected.

5. Select the release to be copied and click **Continue**.

   The system displays the **Copy in Progress** screen.

Copy in Progress screen



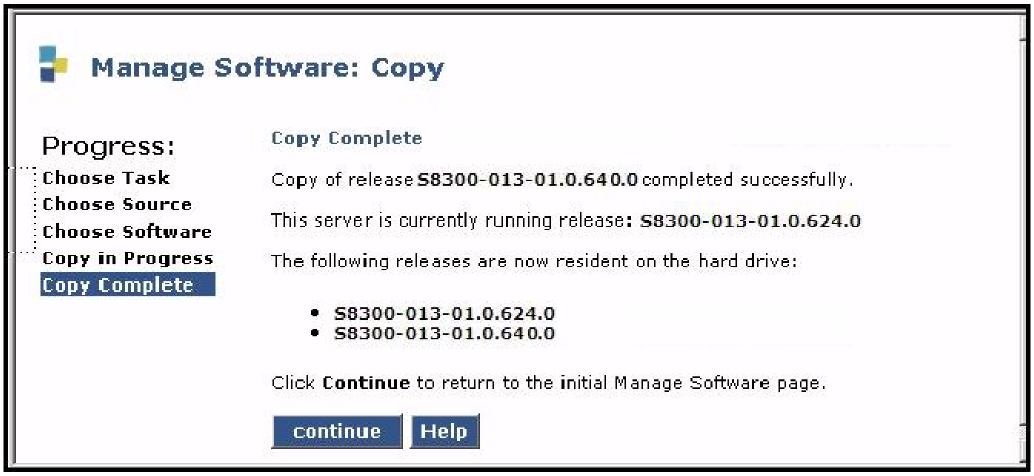
Copy in Progress

1206 files are being copied.
The output of the copy sequence so far is:

```
11:46:05 | [205] 014-tcpdump-3.6.3.17.8.0.3.i386.rpm
11:46:05 | [206] 014-telnet-server-017-23.i386.rpm
11:46:06 | [207] 014-tftp-server-0.29-3.i386.rpm
11:46:08 | [208] 014-timeconfig-3.2.9-1.i386.rpm
11:46:14 | [209] 014-usermode-1.63-1.i386.rpm
11:46:15 | [210] 014-util-linux-2.11r-10.i386.rpm
11:48:18 | [211] 014-vixie-cron-3.0.1-69.i386.rpm
11:46:19 | [212] 014-vsftpd-1.1.001.i386.rpm
11:46:20 | [213] 014-xdelta-1.1.3-7.i386.rpm
11:46:21 | [214] 014-xinetd-2.3.11-1.8.0.i386.rpm
```

The screen lists each file as it is being copied to the S8300 hard drive. When the copy completes successfully, the **Copy Complete** screen appears.

Copy Complete screen



Copy Complete

Copy of release S8300-013-01.0.640.0 completed successfully.

This server is currently running release: S8300-013-01.0.624.0

The following releases are now resident on the hard drive:

- S8300-013-01.0.624.0
- S8300-013-01.0.640.0

Click **Continue** to return to the initial Manage Software page.

This screen indicates the release just copied, shows the release running on the S8300, and shows the releases resident on the server's hard drive.

CAUTION:

If you used the laptop running the tftp server application to copy the software release files from the CD to the S8300 server, at this point you are finished with the software CD-ROM. Remove the CD from your laptop now to avoid possible problems the next time your laptop is rebooted.

Upgrade the S8300

This section describes the procedures to upgrade the S8300B or S8300C Server from a 2.x, 3.x, 4.x, or 5.0 - 5.1.x release of Communication Manager to release 5.2. To upgrade from a pre-2.0, use the procedures in Chapter 7: Migrating an S8300 Server on page 351. The coresident SES software is automatically installed along with Communication Manager software. For the customer to use SES, you must enable SES and install a separate SES license later.

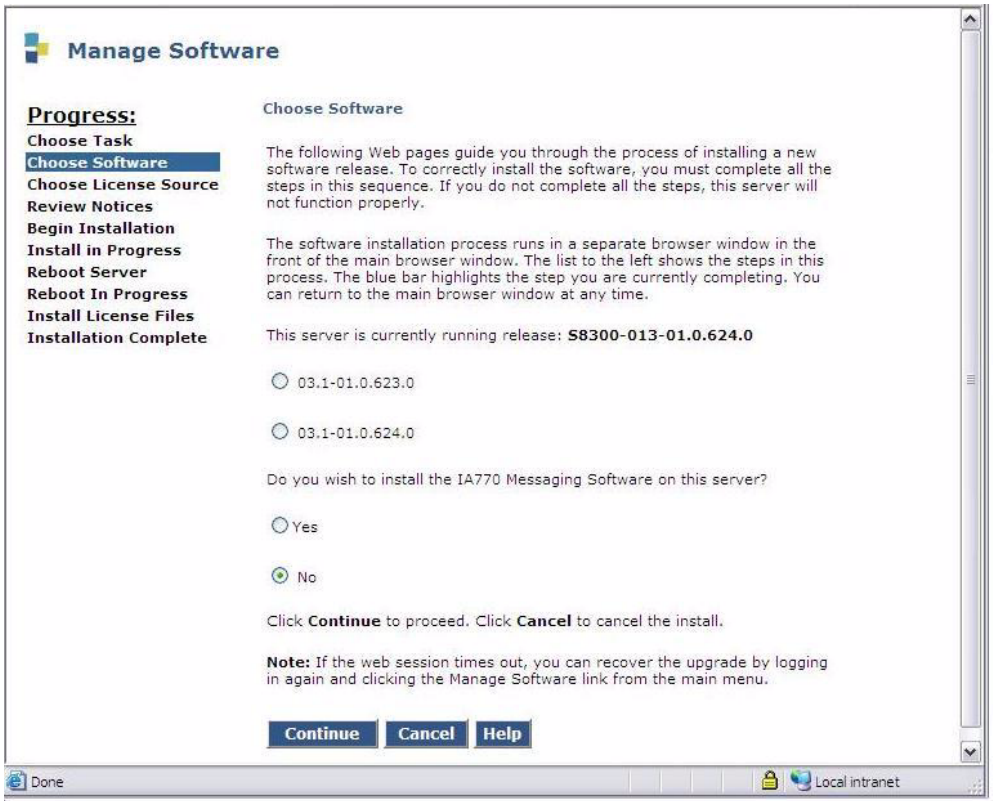
Installing new software

The first step in upgrading the S8300B or S8300C Server to Communication Manager 5.2 is to copy the appropriate software release to the server hard drive using the Manage Software screens of the Web Interface (see Copying the software and firmware files to the server on page 323). The next step is installation of the new release, which is now resident on the S8300.

1. After you have finished with the **Copy Complete** screen, click **Continue**.

   The **Choose Software** of the **Manage Software: Install** screen appears.

Choose Software screen



Manage Software

Progress:
Choose Task
Choose Software
Choose License Source
Review Notices
Begin Installation
Install in Progress
Reboot Server
Reboot In Progress
Install License Files
Installation Complete

Choose Software

The following Web pages guide you through the process of installing a new software release. To correctly install the software, you must complete all the steps in this sequence. If you do not complete all the steps, this server will not function properly.

The software installation process runs in a separate browser window in the front of the main browser window. The list to the left shows the steps in this process. The blue bar highlights the step you are currently completing. You can return to the main browser window at any time.

This server is currently running release: **S8300-013-01.0.624.0**

○ 03.1-01.0.623.0

○ 03.1-01.0.624.0

Do you wish to install the IA770 Messaging Software on this server?

○ Yes

● No

Click **Continue** to proceed. Click **Cancel** to cancel the install.

Note: If the web session times out, you can recover the upgrade by logging in again and clicking the Manage Software link from the main menu.

This screen shows the release currently running on the S8300, and the releases resident on the hard drive. To install the 5.x release, select the radio button next to the 5.x release and click **Continue**.

This screen also displays a prompt for installing Communication Manager Messaging.

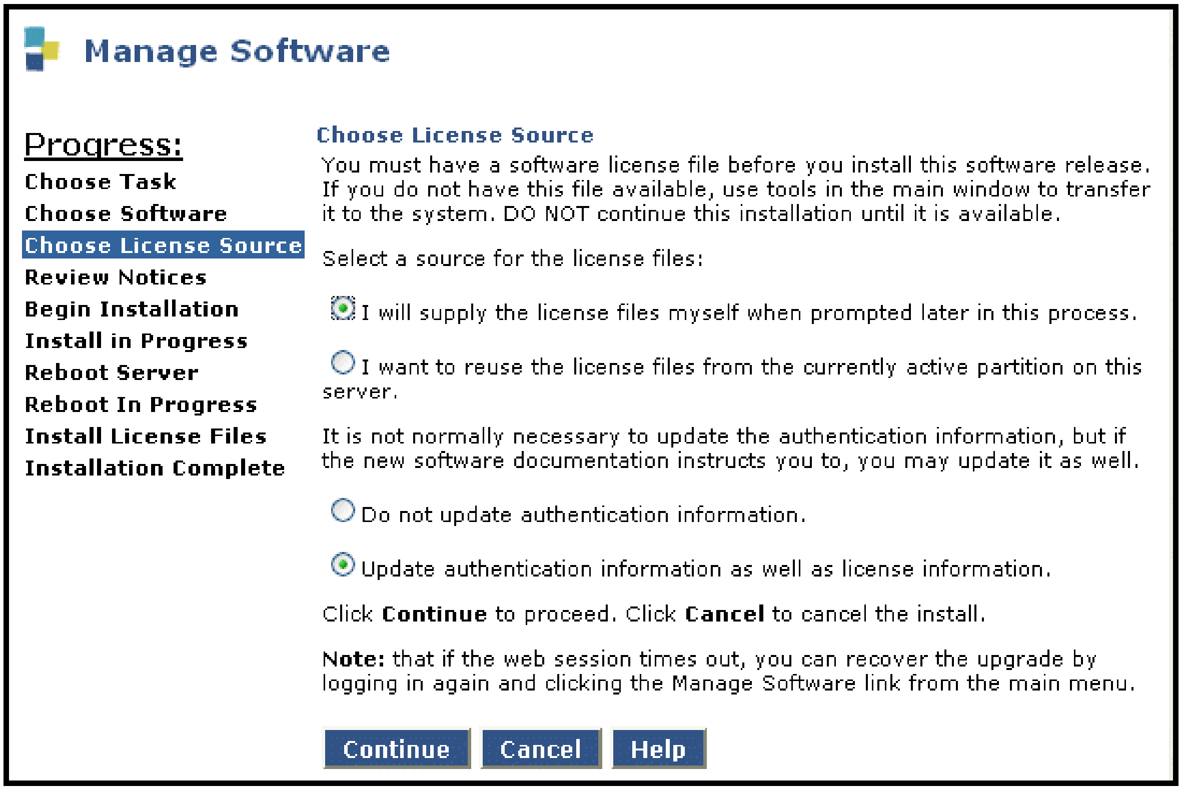
The radio buttons default as follows: If Communication Manager Messaging is not supported, the "no" button will be selected; if Communication Manager Messaging is supported, the "yes" button will be selected.

The install screens following the Communication Manager Messaging screen are unchanged from their former versions.

2. Click **Continue**.

   The S8300 displays the **Choose License Source** screen.

Choose License Source screen



Choose License Source

You must have a software license file before you install this software release. If you do not have this file available, use tools in the main window to transfer it to the system. DO NOT continue this installation until it is available.

Select a source for the license files:

● I will supply the license files myself when prompted later in this process.

○ I want to reuse the license files from the currently active partition on this server.

It is not normally necessary to update the authentication information, but if the new software documentation instructs you to, you may update it as well.

○ Do not update authentication information.

● Update authentication information as well as license information.

Click **Continue** to proceed. Click **Cancel** to cancel the install.

Note: that if the web session times out, you can recover the upgrade by logging in again and clicking the Manage Software link from the main menu.

3. For a typical upgrade, the Communication Manager license and authentication files, if required, should be copied to the server as described in Copying Files to the S8300 hard drive on page 322, so that the files are automatically installed during the upgrade process running under the control of Manage Software web page. If these files are not copied to the server, copy the files to the server before you upgrade.

   If you want the upgrade process to automatically install the license and authentication file, select the following:

   - I want to reuse the license files from the currently active partition on this server.
   - Do not update authentication information.

   If you want to install the license and authentication file after the upgrade using the Installing updated Communication Manager license and authentication files on page 333 procedure, select the following:

   - I will supply the license/authentication files myself when prompted later in this process.
   - Update authentication information as well as license information.

4. Click **Continue**.

   The system displays the **Review Notices** screen.

5. For a new installation, or if you previously ran a backup as described in Backing up data on the S8300 Server on page 316, you do not need to run a backup at this time.

   If your planning documents instruct you to enable Tripwire, follow the instructions to reset the signature database.

6. Click **Continue**.

   The S8300 displays the **Begin Installation** screen, which summarizes the request you have made.

7. Click **Continue**.

   The S8300 displays the **Install in Progress** screen.

   The installation should take 10 to 20 minutes.

8. Click **Reboot**.

   If IA770 is being used, it may take approximately 5 minutes to shut down Communication Manager Messaging before the reboot begins.

   The S8300 displays the **Reboot in Progress** screen.

   Note:

   > The reboot can take 20 minutes or longer. The system does not automatically tell you when the reboot is complete.

9. Wait 5 minutes and then click **Continue**.

   Note:

   > If you click Continue before the reboot is finished, you see **Expired Page** on the screen. If you see the Expired Page message, refresh the browser. If the Session Timeout screen appears, close the screen, logoff, and log on again, return to the **Manage Software** page, and select **Join this upgrade session in progress and monitor its activity**, and click **Continue**. The system displays the **Reboot in Progress** screen.

   Note:

   > The Web session is interrupted by the reboot that occurs during the upgrade of the primary server. After the reboot, you can continue to use the **Manage Software** window without logging in.

10. When the reboot is complete, clicking **Continue**.

    The system displays the **Update Tripwire Database** screen. Unless instructed in your planning documents to update the tripwire database, select **Do not update the tripwire data base now**

11. Click **Continue**.

- If at step 3, you chose I want to reuse the license file, the system displays the **Installation Complete** screen.

- If at step 3, you chose I will supply the license files myself when prompted, the system displays the **Install License Files** screen. Click **Continue**.

  Note:

  The system may perform a Communication Manager process restart to complete the license installation.

  The system displays the **Installation Complete** screen. Observe the Installation Complete screen for additional information.

12. Click **Close**.

The **Installation Complete** screen and the **Manage Software** Web page close. You are returned to the Integrated Management Maintenance Web Pages.

Note:

Depending on the software running prior to the upgrade, the Integrated Management Web session opened prior to the upgrade may be unusable. If you observe the message: *Inconsistent menus detected in the current session*. This could be due to a recent upgrade, and so on. If the problem is persistent with the current session, please close all Web browsers associated with this session and log in again. You must close and reopen the Web browser.

You are returned to the main menu.

13. Under Server, click **Software Version** to verify the new software version.

⚠ **Important:**

After upgrading an S8300, you must upgrade the media gateway and media module firmware before restarting Communication Manager Messaging.

Installing updated Communication Manager license and authentication files

⚠ **CAUTION:**

A super-user login or dadmin login must exist *before* you install an authentication file. If the authentication file does not install, you might need to create a super-user login, then install the new authentication file. See Ensuring a super-user login exists on page 300.

Note:

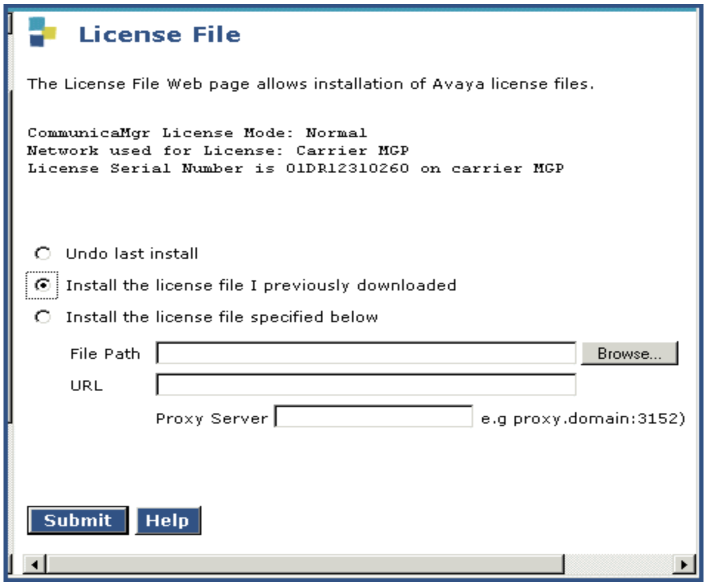
If SES is to be enabled, you install the SES license later using the WebLM screen through the SES administration interface.

To install the license and authentication files:

1. On the **Server (Maintenance)** Web page, select **Security** > **License File**.

   The **License File** screen appears.

License File Screen



License File

The License File Web page allows installation of Avaya license files.

```
CommunicaMgr License Mode: Normal
Network used for License: Carrier MGP
License Serial Number is 01DR12310260 on carrier MGP
```

○ Undo last install

● Install the license file I previously downloaded

○ Install the license file specified below

File Path

URL

Proxy Server e.g proxy.domain:3152)

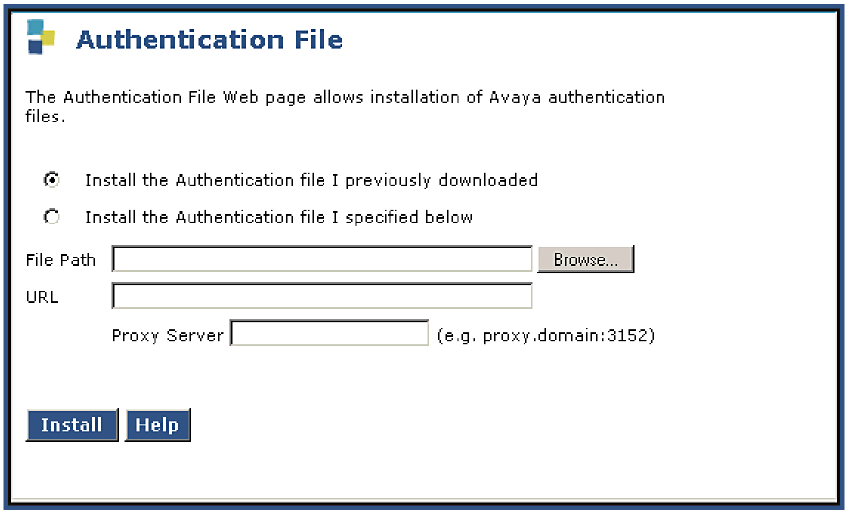
2. Select **Install the license file I previously downloaded** and click **Submit**.

   The system informs you the license has been installed successfully.

3. Under Security, select **Authentication File**.

   The **Authentication File** screen appears.

Authentication File screen



Authentication File

The Authentication File Web page allows installation of Avaya authentication files.

● Install the Authentication file I previously downloaded

○ Install the Authentication file I specified below

File Path

URL

Proxy Server (e.g. proxy.domain:3152)

4. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system tells you the authentication file is installed successfully. If the authentication file does not install, you may need to add a super-user login first. See Ensuring a super-user login exists on page 300.

If the server is an LSP, stop and start Communication Manager

Note:

Skip this task if the Communication Manager processes were already stopped and started after the license file installation.

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`.
3. Type `start -ca`.

If upgrading an S8300C LSP, configuring the LSP for compatibility with an XL configuration

Note:

If the primary controller is an S8720 or S8730 configured as XL the LSP must be an S8300C and must be configured as XL. The S8300B cannot be an LSP for a primary server configured as XL.

To configure the S8300C LSP to be compatible with the *main* S8720 in XL configuration or the *main* S8730 Server:

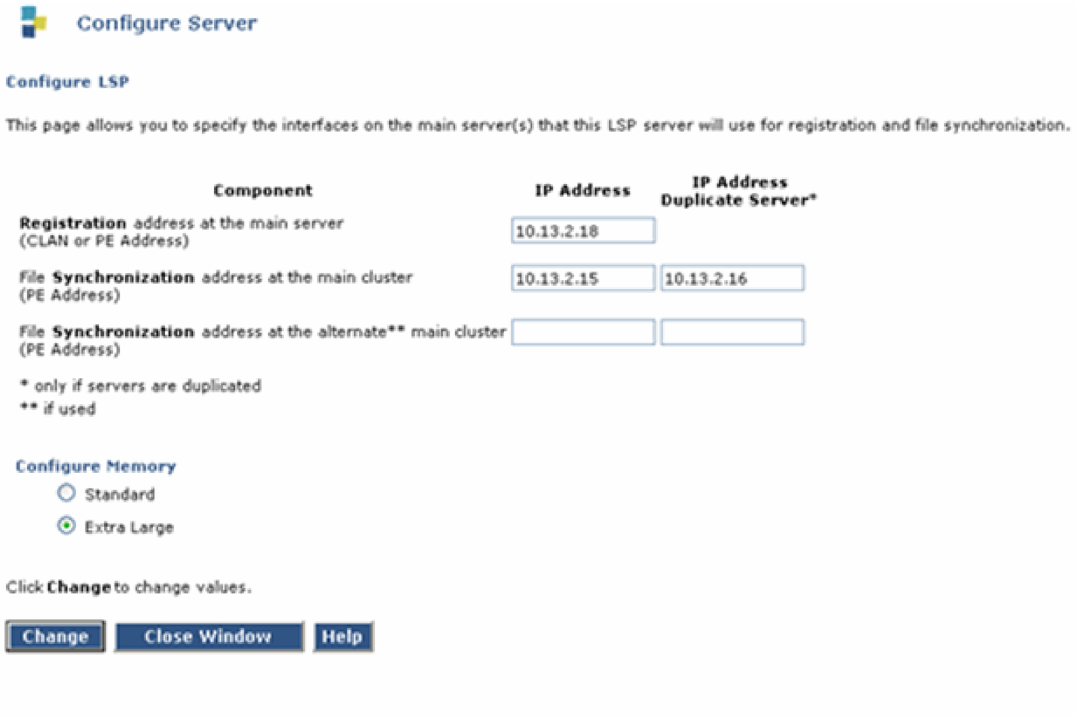
1. At the server command line interface, type `stop -acfn` and press **Enter** to stop Communication Manager call processing.
2. On the Communication Manager System Management Interface main Web page, from the **Installation** menu, click **Configure Server**.

   The system displays the **Review Notices** screen.
3. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.

⚠ **CAUTION:**

For the next step, if you select and save as **Extra Large** you cannot revert to **Standard**. If you try to go back to **Standard**, server translation corruption occurs.

4. Select **Configure individual services** and click **Continue**.
5. In the left column, click **Configure LSP**.



Configure Server

Configure LSP

This page allows you to specify the interfaces on the main server(s) that this LSP server will use for registration and file synchronization.

Component	IP Address	IP Address Duplicate Server*
Registration address at the main server (CLAN or PE Address)	10.13.2.18	
File **Synchronization** address at the main cluster (PE Address)	10.13.2.15	10.13.2.16
File **Synchronization** address at the alternate** main cluster (PE Address)		

* only if servers are duplicated
** if used

Configure Memory

○ Standard
● Extra Large

Click **Change** to change values.

6. Select **Extra Large** and click **Change**.
7. Click **Close Window**.
8. At the server command line interface, type `start -ac` and press **Enter** to restart Communication Manager call processing.
9. At the server command line interface, type `swversion` and press **Enter**.
10. In the **Memory Config** field, verify that the setting is **Extra Large**.If

Installing security updates, Communication Manager service pack updates, and SES service pack updates, if any

To install update files

1. Under Server Upgrades, select **Manage Updates**.

   The **Manage Updates** screen appears.

2. If an update file you want to activate shows **packed** in the **Status** column, select the file in the **Update ID** column, and click **Unpack**.

   The window shows the status of the unpacking.

3. Wait until the system displays the message `...unpacked successfully` and click **Continue**.

   The system displays the **Manage Updates** screen.

4. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

   The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

5. Click **Yes**.

   Wait until the system displays the Continue button.

6. Click **Continue**.

Install the SES license

Note:

Skip this task if SES will not be enabled for this S8300 server. SES cannot be enabled on an S8300 LSP. SES cannot be enabled on an S8300B.

Install the SES license from the WebLM server that is located on an edge or a combined home/ edge server:

1. On the Communication Manager System Management Interface Web page, under **Administration**, click **SIP Enablement Services**.

2. Select **Server Configuration** > **License**.

   The **List Licenses** page displays.

3. Click **Access WebLM**.

   The **WebLM** application screen displays in a new window.

4. If this is the first time the application has run, you must log in with "admin" as the default login and "weblmadmin" as the default password, then change both the default login and password to the customer's preferences for this account.

Note:

If the WebLM server is on a different subnet than the server, you must change the URL in your browser to include the server's DNS name. When you mouse-over the WebLM link on the List Licenses page, the URL includes an IP address, for example, "https://12.34.56.78/WebLM/index.jsp/" Change the URL to "https://server-name/WebLM/index.jsp/", where server-name is the DNS name of the server on which you want to install the SES license.

5. Select **License Administration**.

   The **authentication** screen displays.

6. Login as **admin** and enter the password.

   After this initial login, the system prompts you to change the password.

7. Change the password.

   WebLM logs you out.

8. Log in again as **admin** with the newly-created password.

   The **Web License Manager (WebLM)** screen displays.

9. Select **Install License**.

   The **Install License** page displays.

10. Click **Browse** to navigate to the SES license that you want to install.

11. Click **Install**.

    If the license is valid, the system indicates that it was installed successfully; otherwise the process fails with a brief description

Note:

> The license update for the home seats can take up to 15 minutes. Wait approximately 15 minutes before continuing with verifying the license installation (Step 12).

12. To verify the license installation go to the Integrated Management SIP Server Management Top page and select **Server Configuration** > **License**.

    The **List Licenses** page displays.

13. Ensure that the following three (3) licenses are listed in the Name column:

    - Edge Proxy

    - Basic Proxy

    - Home Seats

14. Click **Show by the Edge Proxy listing**.

    The **License Information** page displays.

15. Ensure that the page displays the following information:

    ```
    Proxy Name sipserver

    Requested 1

    Acquired 1
    ```

16. Click **Show by the Basic Proxy listing**.

    The **License Information** page displays.

17. Ensure that the page displays the following information:

    ```
    Proxy Name sipserver
    Requested 1
    Acquired 1
    ```

18. Click **Show by the Home Seats listing**.

    The **License Information** page displays.

19. Ensure that the page displays the following information:

    ```
    Proxy Name sipserver
    Requested XXX
    Acquired XXX
    ```

    where XXX is the actual number of seats in the license.

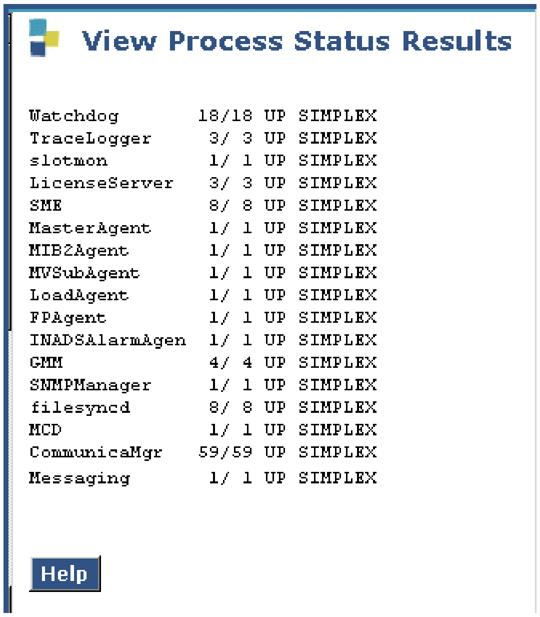
If Communication Manager Messaging has been upgraded, verify messaging has started

If you installed Communication Manager Messaging, the messaging application should start after you install the license. To verify that messaging has started, perform the following steps:

1. On the **Server (Maintenance)** Web page, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

   The **View Process Status Results** screen appears.

View Process Status screen



```
Watchdog        18/18 UP SIMPLEX
TraceLogger      3/ 3 UP SIMPLEX
slotmon          1/ 1 UP SIMPLEX
LicenseServer    3/ 3 UP SIMPLEX
SME              8/ 8 UP SIMPLEX
MasterAgent      1/ 1 UP SIMPLEX
MIB2Agent        1/ 1 UP SIMPLEX
MVSubAgent       1/ 1 UP SIMPLEX
LoadAgent        1/ 1 UP SIMPLEX
FPAgent          1/ 1 UP SIMPLEX
INADSAlarmAgen   1/ 1 UP SIMPLEX
GMM              4/ 4 UP SIMPLEX
SNMPManager      1/ 1 UP SIMPLEX
filesyncd        8/ 8 UP SIMPLEX
MCD              1/ 1 UP SIMPLEX
CommunicaMgr    59/59 UP SIMPLEX
Messaging        1/ 1 UP SIMPLEX
```

3. Make sure Messaging shows **UP**.

   The number of processes (59/59) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 58/59 UP would indicate that a process did not come up and should be investigated before proceeding.

   If you need to start messaging, you can use either the Maintenance Web pages or the Linux command line. For the Maintenance Web pages, see Starting Communication Manager Messaging with the Messaging Web pages, if necessary on page 340. For the Linux command line method, see Starting Communication Manager Messaging with the command line, if necessary on page 341.

Starting Communication Manager Messaging with the Messaging Web pages, if necessary

1. On the **Server (Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The Messaging Administration Web page is displayed in a new Web browser window.

2. From the Messaging Administration Web page, under **Utilities**, select **Start Messaging**.

   The Start Messaging Software Web page is displayed. This page will display the status of the system as it starts.

3. When the message `End start_vm: voice messaging is now completely up` is displayed, select the **Return to Main** button and do the next procedure in this document.

Starting Communication Manager Messaging with the command line, if necessary

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type **`start -s Audix`**
3. Ensure that all Communication Manager processes come up.

   To monitor the startup of Communication Manager Messaging:

   a. Type **`watch /VM/bin/ss`**

      The display will periodically refresh automatically. When you see the following display, the Communication Manager Messaging startup is complete.

   b. Press **Ctrl+C** to break out of the **`watch`** command.

Testing to verify system functionality

Test the system for functionality by verifying the following:

- Telephones have dial tone
- You can call from one telephone to another telephone on the system
- You can make an external trunk call.
- The media gateways have registered. Use the SAT command **`list media-gateway`**.

Making the upgrade permanent

⚠ **CAUTION:**

You must make the upgrade of the software permanent so that the software is recognized and kept on the S8300. If you fail to make software permanent, then the next time you reboot, old software will become active.

To make the upgrade permanent

1. From the Maintenance Web Interface main menu, under Server Upgrades, click **Make Upgrade Permanent**.

   The S8300 displays the **Make Upgrade Permanent** window.

2. Click **Submit**.

   When the new S8300 upgrade software is permanent, the S8300 displays the following message:

   ```
   The commit operation completed successfully
   ```

Saving translations

Note:

If the S8300 you are upgrading is an ***LSP***, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session and log in as *craft* (or *dadmin*).
2. If the S8300 you are upgrading is a primary controller, at the SAT prompt, type **`save translation`** and press **Enter**.
3. If the S8300 you are upgrading is an LSP, then on the primary controller, type **`save translation lsp`** and press **Enter**. This command distributes saved translations out to the LSPs.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

   The LSP automatically performs a reset system 4.

If Communication Manager Messaging fails to start after an upgrade

If you have upgraded your Communication Manager and Communication Manager Messaging software, you must have a new license that is associated with the latest release. Communication Manager Messaging will not use the license for a previous version.

If you upgraded Communication Manager Messaging without a new license file, it will fail to start during the Communication Manager startup sequence.

If this occurs, you must perform the following steps:

1. Obtain an Communication Manager Messaging license file.
2. Install the license file.
3. From a command prompt, start the Communication Manager Messaging process with the following command:

   ```
   start -s Audix
   ```

Copying IP Phone firmware to the server, if necessary

If, before the upgrade, the server was serving as an http server for IP phone firmware, download the most recent IP phone firmware bundle available from the Avaya Firmware Download Web site. The firmware bundle reinstates the 46xx IP Phone Web page in Communication Manager and also makes the 46xx IP Phone firmware for the tftp or http server capability of the server.

Note:

The IP phone firmware that was originally downloaded will have been overwritten.

To copy files to the server:

1. On the **Server (Maintenance)** Web page, under **Miscellaneous**, select **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server.**
3. Click **Browse** next to the top field to open the **Choose File** window on your computer. Find the files that you need to copy to the server.
4. Click **Install this file on the local server**.
5. Click **Download** to copy the file(s) to the server.

   The files are copied automatically to the /tftpboot directory.

Installing IP phone firmware download configuration file

Note:

Skip this task if the S8300 server was running Communication Manager release 3.1.3 (R013x.01.3.640.2) or later.

Perform this procedure if the S8300 server is being used to support firmware downloads to IP telephones, and if the S8300 Server was running 3.1.2 (R013.01.2.632.1) or earlier release of software prior to the upgrade.

Use the following steps to restore the 46xxsettings.txt file to the S8300C Server:

1. Use FTP or SFTP or the Download Files page of the System Management Interface to move the 46xxsettings.txt file to the S8300 Server. The file is transferred to the `/var/home/ftp/pub` directory.
2. At the server command line interface, type `cp /var/home/ftp/pub/46xxsettings.txt /tftpboot`.

Upgrading the Firmware on a Media Gateway

Depending on the media gateway in which the S8300 Server is mounted, the steps requried to upgrade the firmware may vary. Determine the firmware files that are to be installed on the media gateway.

Additionally, you may also need to upgrade the firmware for the media modules.

For more information on the firmware upgrade process on a G700 Media Gateway, see *Installing and Upgrading the Avaya G700 Media Gateway*, 03-603333.

For more information on the firmware upgrade process on a G250 Media Gateway, see *Installing and Upgrading the Avaya G250 Media Gateway for CM 3.1*, 03-300434.

For more information on the firmware upgrade process on a G350 Media Gateway, see *Installing and Upgrading the Avaya G350 Media Gateway.*

For more information on the firmware upgrade process on a G430 Media Gateway, see *Installing and Upgrading the Avaya G430 Media Gateway*, 03-603233.

For more information on the firmware upgrade process on a G450, see "Upgrading the G450 Firmware" in the *Installing and Upgrading the Avaya G450 Media Gateway*, 03-602054.

For more information on the IG550 Integrated Gateway, see *Installing and Configuring the Avaya IG550 Integrated Gateway*, 03-601554.

Note:

For Release 5.2 of Communication Manager the use of Upgrade Tool is eliminated.

Post-upgrade tasks

After the upgrade is complete, perform the following post-upgrade tasks.

Stopping Communication Manager Messaging, if loading an Communication Manager Messaging update

After the upgrade is complete, perform the following post-upgrade tasks:

1. On the **Server (Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, under **Utilities**, select **Stop Messaging**.

   The **Stop Messaging Software** Web page is displayed.

3. Select the **Stop** button.

   The shutdown of the messaging server will begin when all users have logged off from Communication Manager Messaging or after three minutes have passed, whichever event comes first. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing Communication Manager Messaging service pack (or RFU) files, if any

If Communication Manager Messaging is being used, a post-upgrade service pack for Communication Manager Messaging may be required. See the Communication Manager Messaging documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at http://support.avaya.com.

1. Select **Messaging Administration** from the main menu.
2. Under **Software Management,** select **Adv Software Installation**.
3. Select **Continue this operation without current system backup**.
4. Select the Communication Manager Messaging update package and click **Install Selected Packages**.

   Note:

   > The system automatically prompts you to restart CM Messaging when the service pack has been installed. Therefore, if you restart CM Messaging at this time, you do *not* need to perform the following procedure, Starting Communication Manager Messaging on page 346.

Starting Communication Manager Messaging

⚠ **CAUTION:**

> You do *not* need to perform this task if you restarted Communication Manager Messaging as a part of the installation of the Communication Manager Messaging service pack.

After the Communication Manager Messaging application has been updated, you must restart it using the following steps:

1. On the **Server** (**Maintenance)** Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, under **Utilities**, select **Start Messaging**.

   The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

3. When the message `End start_vm: voice messaging is now completely up` is displayed, close the Messaging Administration Web page and perform the next procedure in this document.

Verifying start up of Communication Manager Messaging

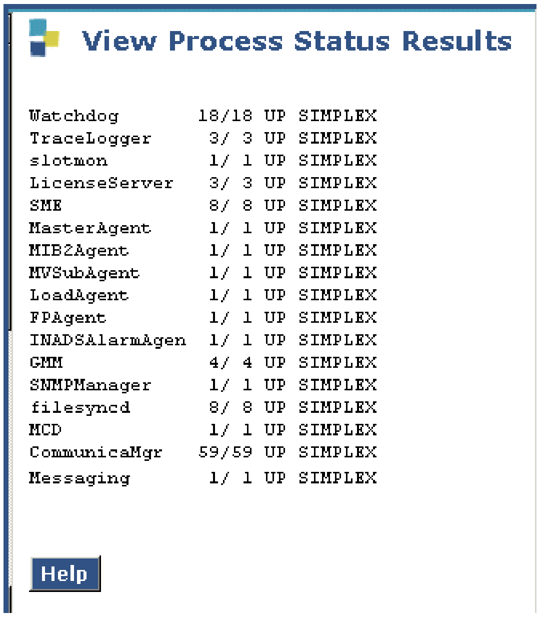
To verify operation of Communication Manager Messaging, perform the following steps:

1. On the **Server (Maintenance)** Web page, under Server, click **Process Status**.

2. Select **Summary and Display once** and click **View**.

   The **View Process Status Results** screen appears.

View Process Status screen



View Process Status Results

```
Watchdog        18/18 UP SIMPLEX
TraceLogger      3/ 3 UP SIMPLEX
slotmon          1/ 1 UP SIMPLEX
LicenseServer    3/ 3 UP SIMPLEX
SME              8/ 8 UP SIMPLEX
MasterAgent      1/ 1 UP SIMPLEX
MIB2Agent        1/ 1 UP SIMPLEX
MVSubAgent       1/ 1 UP SIMPLEX
LoadAgent        1/ 1 UP SIMPLEX
FPAgent          1/ 1 UP SIMPLEX
INADSAlarmAgen   1/ 1 UP SIMPLEX
GMM              4/ 4 UP SIMPLEX
SNMPManager      1/ 1 UP SIMPLEX
filesyncd        8/ 8 UP SIMPLEX
MCD              1/ 1 UP SIMPLEX
CommunicaMgr    59/59 UP SIMPLEX
Messaging        1/ 1 UP SIMPLEX
```

3. Make sure Messaging shows **UP**.

   The number of processes (59/59) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 58/59 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an Communication Manager Messaging sanity test:
   a. At the Linux command line, type **`/vs/bin/display`**.
   b. All states should be `Inserv` with an associated phone number.
   c. Retrieve the test message saved before the upgrade.
6. At the Linux command line, type **`/VM/bin/ss`**.
7. Verify that all Communication Manager Messaging processes are shown.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.

3. Type **`save translation all`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

If using Communication Manager Messaging, administering switch integration for H.323

The Communication Manager Messaging application uses H.323 signaling instead of the CWY1 board for integration with Communication Manager. The tasks for administering the H.323 integration are explained in *Administering Media Servers to Work with IA770*.

Testing to verify system functionality

If you are upgrading an S8300 primary controller, test the system for functionality.

1. Verify the following:
   - Telephones have dial tone
   - You can call from one telephone to another telephone on the system
   - You can make an external trunk call.
   - The media gateways have registered. Use the SAT command **`list media-gateway`**.

Completing the upgrade process (S8300 is the primary controller)

Telnet to the S8300 (primary controller) and open a SAT session to perform the following:

1. To check media modules on page 349
2. To enable scheduled maintenance on page 349
3. To busy out trunks on page 349
4. To check for translation corruption on page 349
5. To resolve alarms on page 349
6. To re-enable alarm origination on page 349

To check media modules

1. Type **`list configuration all`** and press **Enter**.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that Communication Manager is working.

To enable scheduled maintenance

1. Type **`change system-parameters maintenance`** and press **Enter**.
2. Ensure that the **Start Time** and **Stop Time** fields' administration is the same as before the upgrade.

To busy out trunks

1. Busy out trunks that were busied out before the upgrade (see To record all busyouts on page 309).

To check for translation corruption

1. Type **`newterm`** and press **Enter**.

   If you do not get a login prompt and the following message appears,

   ```
   Warning: Translation corruption detected
   ```

   follow the normal escalation procedure for translation corruption before continuing the upgrade.

To resolve alarms

1. In the Maintenance Web Interface, under Alarms click **Current Alarms** to examine the alarm log.
2. If any alarms are listed, click **Clear All**.
3. Resolve new alarms that have appeared since the upgrade through Communication Manager. For instructions see the appropriate maintenance book.

To re-enable alarm origination

1. Telnet to the S8300 and log on.
2. At the command prompt, type **`almenable -d b -s y`**,

   where

   `-d b` sets the dialout option to *both* (numbers)

   `-s y` enables SNMP alarm origination
3. Type **`almenable`** (without any options) to verify alarm origination enabled status.

Backing up the system

To back up the system over the customer's LAN:

1. Make sure you have the IP address of the customer's FTP, SFTP, or SCP backup server.
2. On the S8300 main menu, select **Backup Now**.

   The system displays the **Backup Now** screen.
3. Select the type of data you want to back up by selecting the appropriate data set.
4. Select a backup method, normally **FTP**, **SFTP**, or **SCP**, to indicate the destination to which the system sends the backup data.
5. Complete the following fields:
   - **User name**

     You must enter a valid user name to enable the S8300 Server to log in to the FTP, SFTP, or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.
   - **Password**

     You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.
   - **Host name**

     Enter the DNS name or IP address of the FTP, SFTP, or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).
   - **Directory**

     Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. If you do not want to use the default directory, you must enter the path name for the directory.
6. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

This completes the installation of the media gateway with an S8300 Server as primary controller.

Chapter 7: Migrating an S8300 Server

Overview

This section covers the procedures to migrate the following:

- Avaya S8300A or S8300B Server with an Avaya S8300C Server
- Avaya S8300A or S8300B or S8300C Server with an Avaya S8300D Server

All the steps in this section are applicable to both the migration paths. A few steps in the migration procedure are exclusive to S8300A Server since the S8300A Server runs Communication Manager 1.x or 2.0.x release.

Note:

Starting with Communication Manager release 5.2, IA770 is called Communication Manager Messaging. Instances of IA770 in this section imply that the Communication Manager release is pre-5.2.

Note:

The Avaya S8300D Server will be available after May 2009.

Migration of an Avaya S8300A or S8300B orS8300C Server to an Avaya S8300D Server

Any of the following S8300 Servers running a supported release of Communication Manager can be migrated to S8300D Server:

- S8300C as a Main server
- S8300C as an LSP server
- S8300B as a Main server
- S8300B as an LSP server
- S8300A as a Main server
- S8300A as an LSP server

Supported Communication Manager release for migration

The table provides information about the supported release of Communication Manager on an S8300A or S8300B or S8300C Server in order to migrate to an S8300D Server.

Table 13: Supported Communication Manager releases

Servers	Communication Manager Release									
	1.X	2.0.X	2.1.X	2.2.X	3.0.X	3.1.5	4.0.X	5.0.X	5.1.X	5.2
S8300A	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
S8300B	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
S8300C	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓

Migrating an Avaya S8300A or S8300B Server to an Avaya S8300C Server

You can migrate any of the following S8300 Servers running a supported release of Communication Manager to S8300C Server:

- S8300B as a Main server
- S8300B as an LSP server
- S8300A as a Main server
- S8300A as an LSP server

Supported Communication Manager releases for migration

Ensure that Avaya S8300A or S8300B Server is running a supported release of Communication Manager for migrating to Avaya S8300C Server. For more information, refer to Table 13: Supported Communication Manager releases on page 352.

Before going to the customer site

Complete the steps in the section before you go to the customer site or before starting a remote installation.

Obtaining a USB DVD/CD-ROM drive

Migrating an Avaya S8300A Server or an S8300B Server to an Avaya S8300C Server, or migrating an Avaya S8300A Server, S8300B Server, or S8300C Server to an Avaya S8300D Server requires you to install Communication Manager software on the new server. Therefore, you must have a USB DVD/CD-ROM drive at the site.

There are three external CD/DVD-ROM drives that are supported on the S8300 Server:

- Avaya approved Panasonic Digistor 73082 or 73322 (Comcode: 700406267):
    - The switch must be turned to the ON position.
    - Instead of AC power, the Panasonic Digistor uses a Lithium ION battery for additional power. The CD/DVD-ROM draws more power than the USB port can supply. The additional power required is supplied by the Lithium ION battery. If the Lithium ION battery is depleted, a red LED displays and a f*ailed to mount CD-ROM* message appears. You can charge the Lithium ION battery by plugging the CD-ROM drive in a USB port for approximately 30 minutes. The Lithium ION battery charges faster if the ON/OFF switch is set to OFF.

  Note:

  The functionality of the Lithium ION battery supplying the extra power that the CD/DVD-ROM needs is only applicable for the original CD/DVD-ROM.
- Addonics (Model: AEPDVRWII824) (not available through Avaya):
    - Requires AC power to operate.
    - You must have the switch set to External.
- TEAC (end of sale) (Comcode: 700289580)

Obtaining the serial number of the Media Gateway

The serial number of the media gateway is required to generate the license file.

To get the serial number of the Media Gateway, ask the customer’s administrator to:

1) Log in to the System Management Interface page.

2) Click **Serial Numbers** under **Miscellaneous**.

Note:

The serial number should also be on a sticker on the back of the chassis of the gateway, but this number is occasionally incorrect.

If Communication Manager is being installed for the first time on the server, access the gateway CLI screen and type `show system` command.

Checking the number of allocated ports

With the S8300 Server as a main server, the maximum number of ports is 900.

With the S8300 Server as an LSP, the maximum number of ports could be in thousands as reflected from the main server.

> **CAUTION:**
> If the maximum number of ports exceed 900 for an S8300 Server as a main server, there may be a problem with the upgrade. You need to escalate the issue to your Project Manager.

To check the system for the maximum number of ports, ask the customer to:

1) Log in to the SAT screen.

2) At the SAT command, display `system-parameters customer-options`.

3) Verify that the **Maximum Ports:** field is 900 or less.

Checking the availability of the FTP, SFTP, or SCP Server for backing up data

Before you begin the migration procedure, you can back up the system data to an FTP, SFTP, or SCP Server over the customer's LAN or to a Compact Flash card (only for S8300C or S8300D).

A current version of the system data is required to restore the system configuration after completion of the migration.

- Check with your project manager or the customer for the following information about the FTP Server (Back up to a SFTP, or SCP Server is limited to Communication Manager release 3.1 or later. The back up method available for a release is displayed on the web page):
  - Login ID and password
  - IP address
  - Directory path on the FTP Server

> **Important:**
> Before going to the customer site, make sure that you can use a customer server over the LAN for back ups.

Note:

(S8300C only) You can use an external Avaya approved Compact Flash card and a Card Reader to do the back up for Communication Manager release 4.0 onwards.

On-site preparation for migration

Perform the following tasks before you migrate to S8300C or S8300D Server:

Configuring your laptop

You need to configure your laptop for a direct connection to the services port of the S8300 Server. For more information refer to the **Configuring the laptop for a direct connection** section in the *Installing and Configuring S8300 Server* guide.

Clearing the ARP cache on your laptop

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

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

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

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

Accessing S8300 A/B/C Server

Before you perform migration, you must backup data from the existing server. Thus you will need to connect your laptop to the Services port of the S8300 Server using a crossover cable. For a direct connection to the Services port of the S8300 Server, your laptop must be properly configured.

You will use SSH and the Maintenance Web Interface to perform the procedures. See the following:

- Accessing the server's command line interface with SSH or telnet

Note:

Use of telnet is possible only if the Communication Manager release is 1.X, 2.X, 3.X. For later releases, use SSH.

- Logging in to the S8300 Server's Web Interface from your laptop

Note:

Communication Manager has telnet turned off by default. Therefore, telnet is not available after re-mastering of the hard drive is complete during an initial server installation. However, if the customer later chooses to enable telnet, you may be able to use telnet to access the server's command line interface.

Removing the administration for the IA770 integration if CWY1 board is used (S8300A or S8300B only)

Note:

If the S8300 is configured as an LSP, skip to Checking current software release on page 358.

⚠ **CAUTION:**

Communication Manager Release 5.2 does not support the CWY1 method of integration of IA770. As a result, if the existing S8300 Server uses a CWY1 board to integrate the IA770 application, you must remove IA770 administration now. In addition, you must administer the integration for H.323 after the migration and then administer Communication Manager Messaging

For instructions on removal of existing CWY1 administration, see *Administering Media Servers to Work with IA770*.

Note:

For Releases 2.0 and earlier of Communication Manager that use IA770, you *cannot* remove messaging from the Media Gateway screen in the SAT interface *before* the upgrade. Therefore, you must remove messaging from appropriate slot of the media gateway screen after the upgrade, then administer the H.323 integration.

Saving translations (main only)

If the S8300 Server is an LSP you do not need to save translation. The LSP receives translations from the main server in the event the LSP registers to the main server because of a failure on the main server.

The table lists the releases and corresponding commands to save translations.

Software release of existing media server	Associated software load	Command	Condition
1.2	110.4	save translation	
1.3	526.5	save translation	
1.3.1	531.1	save translation	If LSP present
1.3.2	536.1	save translation	If LSP present
2.0	219.0	save translation	If LSP present
2.0.1	221.1	save translation	If LSP present
2.1	411.1	save translation	If LSP present
2.1.1	414.1	save translation	If LSP present
2.2	111.4	save translation	If LSP present
2.2.1	118.0	save translation	If LSP present
2.2.2	122.0	save translation	If LSP present
3.0 and later	340.3 and later	save translation	If LSP present

Additional Information:

Type `save translation` and `HELP`. If `[all or lsp]` displays, type `save translation all`. Press **Enter**.

Checking current software release

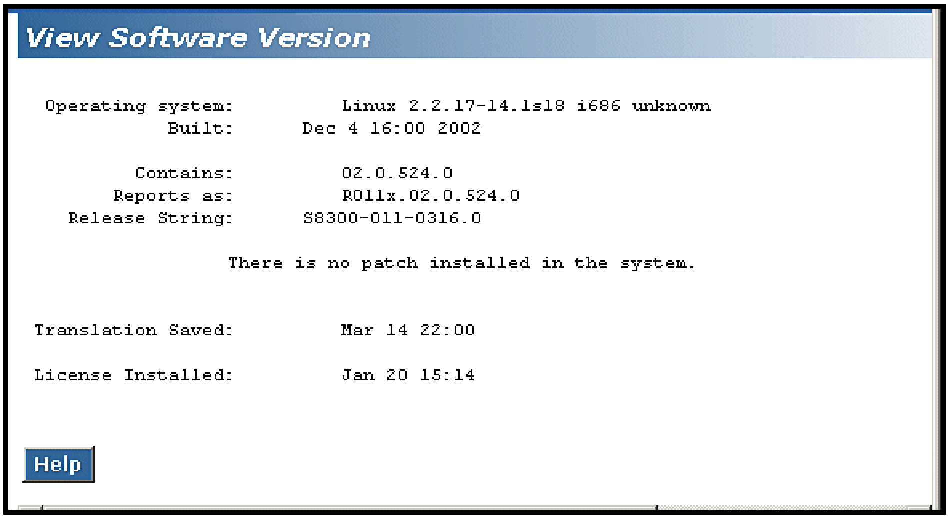
Check the release of Communication Manager currently running on the S8300 to determine whether a pre-upgrade service pack is required. If the current software release requires a pre-upgrade service pack, install the service pack before back up.

To check the current software release

1. Log in to the Web interface on the S8300 and launch the Maintenance Web Interface.
2. Choose **View Software Version** under Server Configuration and Upgrades.

   The system displays the **View Software Version** screen.

Software Version Screen



View Software Version

```
 Operating system:        Linux 2.2.17-14.1s18 i686 unknown
            Built:     Dec 4 16:00 2002

         Contains:        02.0.524.0
       Reports as:        R011x.02.0.524.0
   Release String:     S8300-011-0316.0

                 There is no patch installed in the system.


Translation Saved:        Mar 14 22:00

License Installed:        Jan 20 15:14
```

3. Check the **Reports as:** field for the release number of the S8300 software.
4. Visit http://support.avaya.com/japple/css/japple?temp.documentID=361270&temp.productID=136527&temp.releaseID=348072&temp.bucketID=108025&PAGE=Document to determine if the current software release needs a pre-upgrade patch.
5. On the Web page, under **Pre-Installation Software** you can find a pre-upgrade patch if it is requried for the current release.

Getting IA770 Intuity Audix Messaging application Data (if IA770 is being used)

⚠ **Important:**

Skip to Backing up the S8300A or S8300B or S8300C Server data on page 366 if IA770 is not being used.

If IA770 is being used, you need to collect optional Announcement sets (if this had not been done before arriving at the site), leave a test message, and shut down IA770 before backing up the files.

Determining whether optional languages are needed

To determine the system language

1. On the Server (Maintenance) Web page, under Miscellaneous, select **Messaging Administration**.

   The Messaging Administration Web page appears.

2. Select **Messaging** in the left-hand navigation pane.

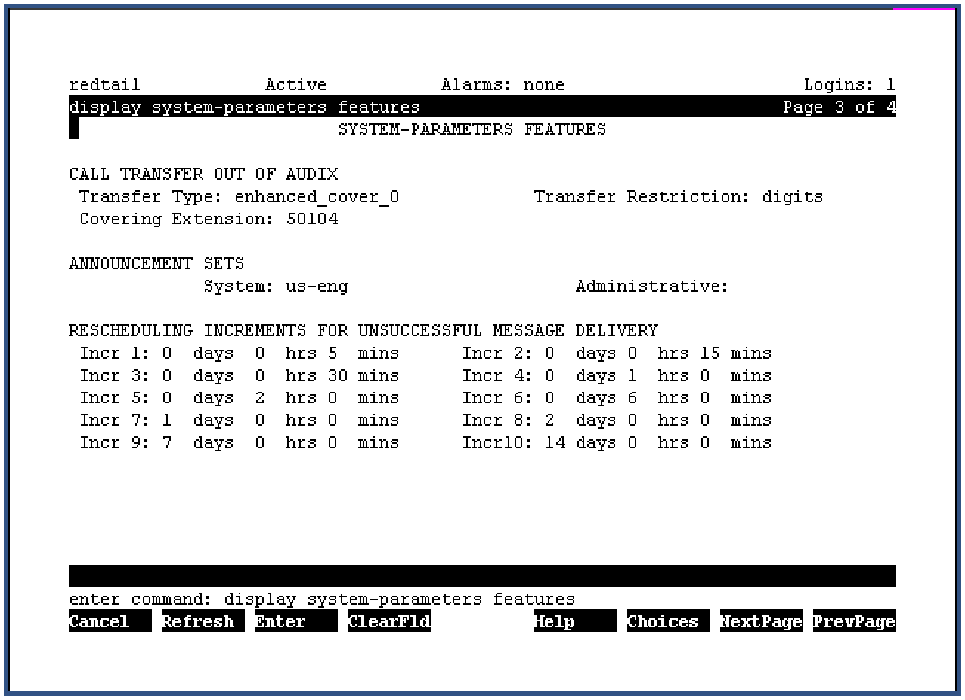
   Security certificates appear.

3. Accept the security certificates.
4. Enter the *craft* password.
5. At the command prompt, enter **display system-parameters features**.

   The **SYSTEM PARAMETERS FEATURES** screen appears.

6. Go to page 3.

System Parameters Features screen, Page 3



```
redtail            Active           Alarms: none                    Logins: 1
display system-parameters features                                  Page 3 of 4
                          SYSTEM-PARAMETERS FEATURES

CALL TRANSFER OUT OF AUDIX
 Transfer Type: enhanced_cover_0            Transfer Restriction: digits
 Covering Extension: 50104

ANNOUNCEMENT SETS
             System: us-eng                      Administrative:

RESCHEDULING INCREMENTS FOR UNSUCCESSFUL MESSAGE DELIVERY
 Incr 1: 0  days  0  hrs 5  mins      Incr 2: 0  days 0  hrs 15 mins
 Incr 3: 0  days  0  hrs 30 mins      Incr 4: 0  days 1  hrs 0  mins
 Incr 5: 0  days  2  hrs 0  mins      Incr 6: 0  days 6  hrs 0  mins
 Incr 7: 1  days  0  hrs 0  mins      Incr 8: 2  days 0  hrs 0  mins
 Incr 9: 7  days  0  hrs 0  mins      Incr10: 14 days 0  hrs 0  mins



enter command: display system-parameters features
```

7. Under **Announcement Sets**, note the main system language listed after **System:** In this example, the main system language is English (**us-eng**). If the system language is anything other than **us-eng** or **us-tdd**, you will need to back up and restore announcement files or reinstall them from a language CD. If the announcement set is customized, you must back up and restore announcement files. See Checking for any Communication Manager Messaging custom announcement sets(R2.0 only) on page 361.

Note:

Starting with release 2.1, only English language files (**us-eng** and **us-tdd**) are included with the Communication Manager software. Before release 2.1, Latin American Spanish and Canadian French (**lat-span** and **french-c**) were also included.

To determine other languages

⚠ **CAUTION:**

> If an announcement package appears on the Web page that follows, that package *must* be present after migration and before you restart messaging. For example, if British English is a package that has been installed, you must back up the package before the migration and restore it after you install Communication Manager release 5.2. If an announcement set present before the migration is not present after the migration, Communication Manager Messaging cannot be restarted.

1. On the Server (Maintenance) Web page, under **Miscellaneous**, select **Messaging Administration**.
2. Under **Software Management**, select **List Messaging Software**.

   The **List Messaging Software** screen appears.
3. Note the **System Announcement** language files listed. In this example, **us-eng** and **us-tdd** are listed. If any language files other than these two are listed, you will need to download the additional language files from a language CD or backup and restore the announcement files.

Checking for any Communication Manager Messaging custom announcement sets(R2.0 only)

Ask the customer if the customer has modified a standard announcement set such as **us-eng** such that the announcement set name is still the standard name. In this case, you must back up the announcement set and restore it after the migration. These steps preserve the custom announcement the customer has created. If the customer has created any customized announcement sets with custom file names, you must back them up and restore them also.

For more information on back up, refer to the Backing up the S8300A or S8300B or S8300C Server data on page 366 section.

Creating an test message for migration

To test Communication Manager Messaging after the migration

1. Write down the number of a test voice mailbox, or create one if none exists.
2. Write down the number of the Communication Manager Messaging hunt group.
3. Leave a message on the test mailbox that will be retrieved after migration.

Shutting down IA770 Intuity Audix Messaging

To shut down IA770 Intuity Audix Messaging

1. On the Maintenance Web page, select **Messaging Administration** from the **Miscellaneous** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. Under **Utilities**, select **Stop Messaging**.

   The **Stop Messaging Software** Web page is displayed.

3. Select the **Stop** button.

   The shutdown of the messaging server will begin when all users have logged off from IA770 or after three minutes have passed, whichever event comes first. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing the pre-upgrade software service pack (if current release is from 1.2.0 through R1.3.0)(

⚠ **Important:**

Visit http://support.avaya.com/japple/css/japple?temp.documentID=361270&temp.productID=136527&temp.releaseID=348072&temp.bucketID=108025&PAGE=Document to determine if the current software release needs a pre-upgrade patch.

Note:

Typically, any existing service pack(s) should be removed before installing a new service pack. However, removing existing service packs is not necessary for this procedure.

To copy a pre-upgrade service pack file to the S8300 Server

If the current software release requires a pre-upgrade patch that is determined from the Avaya support site, you need to copy the pre-upgrade patch to the S8300 Server

1. Make sure the software CD is in the CD-ROM drive of your laptop.
2. On the Server (Maintenance) Web page, under **Miscellaneous**, click **Download Files**.
3. Select the download method **Files to download from the machine I'm using to connect to the server**.

Note:

Do not select the checkbox **Install this file on the local server**.

4. Browse to the directory on the software CD (or laptop) that contains the pre-upgrade service pack file.

5. Select the pre-upgrade service pack file and click **Download**.

Installing the pre-upgrade service pack

Use *one* of the following two procedures to install the pre-upgrade service pack:

- If the current release is 1.x, use To install the pre-upgrade service pack when the current release is pre-2.0. on page 363.
- If the current release is 2.x, use To install the pre-upgrade service pack when the current release is 2.x. on page 364.
- If the current release is 4.x, use To install the pre-upgrade service pack on R4.0 Servers on page 365

To install the pre-upgrade service pack when the current release is pre-2.0.

1. Use Telnet to access the S8300 Server.

   a. Click **`Start > Run`** to open the Run dialog box.

   b. Type **`telnet 192.11.13.6`** and press **Enter**.

   c. Log in as *craft*.

2. Type **`cd /var/home/ftp`** and press **Enter** to access the ftp directory.

3. At the prompt, type **`ls -ltr`** and press **Enter** to list files in the ftp directory.

   The S8300 displays a list of files in the ftp directory.

4. Verify that the directory contains the ***.tar.gz** file you have uploaded.

5. Type **`sudo patch_install`** ***`patch`*****`.tar.gz`** and press **Enter**.

   where ***`patch`*** is the release or issue number of the service pack file. (For example, **`03.1.526.5-1003.tar.gz`**).

6. Type **`patch_show`** and press **`Enter`** to list <replace with long product name> files to verify the new software file was installed.

7. Type **`sudo patch_apply`** ***`patch`*** and press **Enter**.

   where ***`patch`*** is the release or issue number of the service pack file. (For example, **`03.1.526.5-1003`**. Do *not* use the ***.tar.gz** extension at the end of the file name).

   The S8300 Server goes through a software **`reset system 4`**. You must wait until the restart/reset has completed before entering additional commands. The reset should take 1–2 minutes (or longer if messaging is enabled).

8. Type **`patch_show`** again and press **Enter** to list <replace with long product name> files to verify the new software file was applied.

9. Before proceeding, type **`statapp -c`** to view the status of the processes.

   Make sure everything except **dupmgr** shows `UP`. **Communication Manager** should show `65/65 UP` or, if Communication Manager Messaging is installed, `67/67 UP.` To stop the continual refresh of the **`statapp`** command, type **`Ctrl-C`**.

   Note:

   The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before proceeding.

10. Close the telnet session.

To install the pre-upgrade service pack when the current release is 2.x.

Note:

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

The following steps activate the service pack:

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

   The media server may reboot. If it reboots, it also may display the following message:`/opt/ecs/sbin/drestart 2 4 command failed`**.**

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

   The media server displays a message that the service pack was applied.

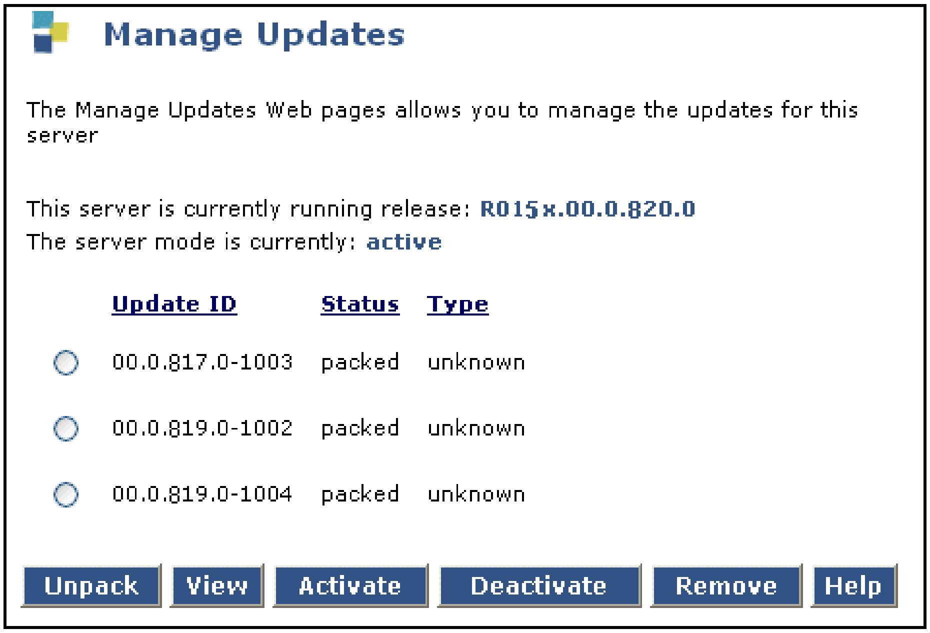
8. Type **`update_show`** again and press **Enter** to list Communication Manager files to verify the service pack file was activated.
9. Enter **y** in response to the question, `Commit this software?`

To install the pre-upgrade service pack on R4.0 Servers

1. Under Server Upgrades, select **Manage Updates**.

   The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allows you to manage the updates for this server

This server is currently running release: R015x.00.0.820.0

The server mode is currently: active

	Update ID	Status	Type
○	00.0.817.0-1003	packed	unknown
○	00.0.819.0-1002	packed	unknown
○	00.0.819.0-1004	packed	unknown

2. If an update file you want to activate shows **packed** in the **Status** column, select update ID and click **Unpack**.

   The window shows the status of the unpacking.

3. Wait until the system displays the message, `... unpacked successfully`, and click **Continue**.

   The system displays the **Manage Updates** screen.

4. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

   The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

5. Click **Yes**.

   Wait until the system displays the **Continue** button.

6. Click **Continue**.

Backing up the S8300A or S8300B or S8300C Server data

The backup procedures are different depending on the software release of Communication Manager currently installed on the server.

Software release of existing media server	Load	Web Interface for Backup	Data Set	File Name
1.2	02.0.110.4	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
1.3	03.0.526.5	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
1.3.1	03.1.531.0	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
1.3.2	03.2.536.1	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.0	00.0.219.0	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.0.1	00.1.221.1	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.1	01.0.411.7	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.1.1	01.1.414.1	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.2	02.0.111.4	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.2.1	02.0.118.1	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
2.2.2	02.2.122.0	Linux Migration Backup/Restore	N/A	upgrade....tar.gz
3.0 and later	00.0.340.3 and later	Backup Now	Full	full....tar.gz

You can back up the S8300-Series Server data by:

- Linux migration backup (if current release is from 1.2.0 through 2.2.2) on page 367
- Backing up the system to compact flash media on page 369

- Backing up the system over the customer's LAN on page 370

Linux migration backup (if current release is from 1.2.0 through 2.2.2)

> **Important:**
> Skip to Backing up the system over the customer's LAN on page 370if the current software release is 3.0 or later.
>
> Skip to Backing up the system to compact flash media on page 369, if the server provides the capability to back up data to a Compact Flash drive.
>
> After the upgrade, you will restore data from the system backup you did earlier.

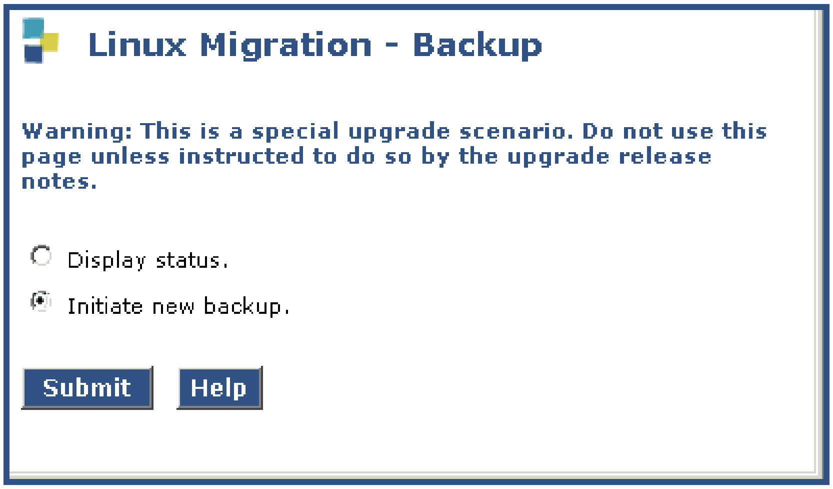
In this section, you use the Linux Migration Backup procedure in the Maintenance Web Interface to save the system files and translations. After the upgrade, you will use the Linux Migration Restore feature to restore these files.

To perform the Linux migration backup

1. Launch the Maintenance Web Interface. Under Server Configuration, click **Linux Migration (Backup/Restore)**.

   The **Linux Migration - Backup** screen appears.

Linux Migration - Backup screen



Linux Migration - Backup

Warning: This is a special upgrade scenario. Do not use this page unless instructed to do so by the upgrade release notes.

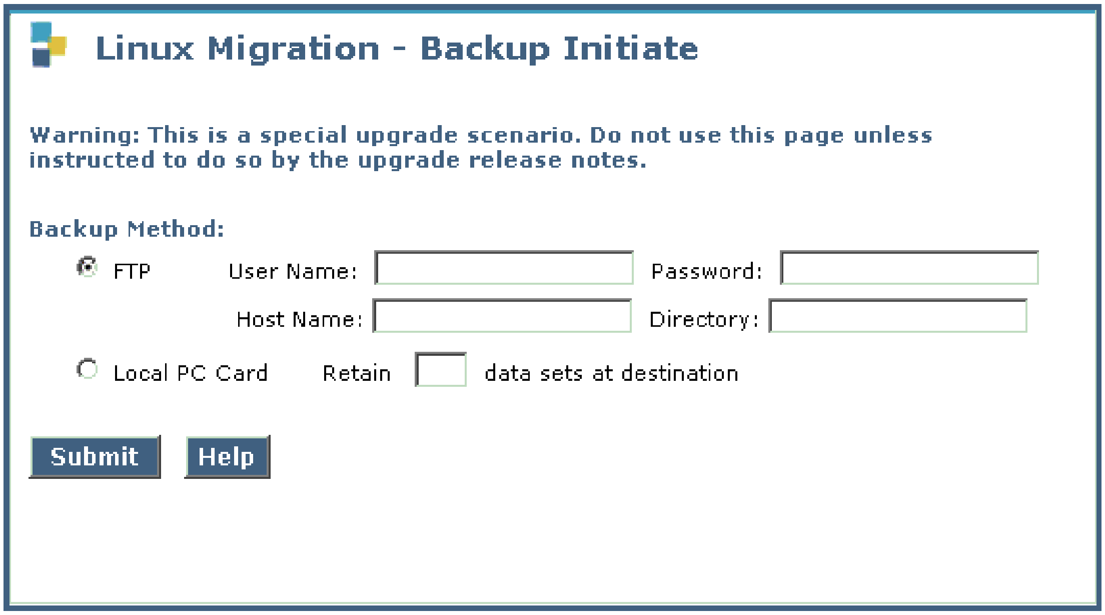
○ Display status.

● Initiate new backup.

2. Select **Initiate new backup or restore** and click **Submit**.

   The **Linux Migration - Backup Initiate** screen appears.

Linux Migration - Backup Initiate screen



Linux Migration - Backup Initiate

Warning: This is a special upgrade scenario. Do not use this page unless instructed to do so by the upgrade release notes.

Backup Method:

● FTP User Name: Password:

Host Name: Directory:

○ Local PC Card Retain data sets at destination

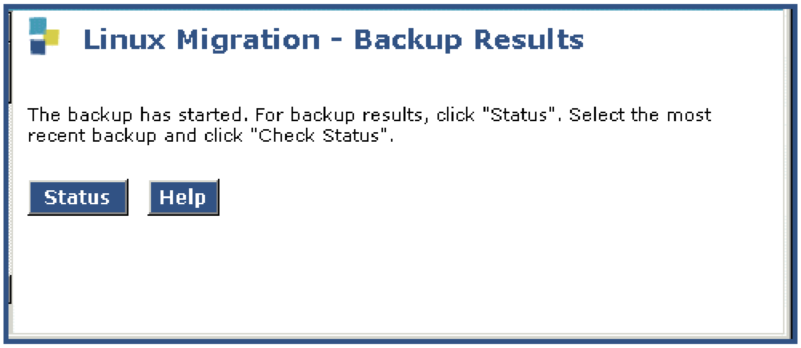
3. Under Backup Method, select FTP.

   Fill in the **User Name**, **Password**, **Host Name (or host IP address)** and **Directory** fields for the back up location. The backup location should be a server on the customer's LAN.

4. Click **Submit**.

   The **Linux Migration - Backup Results** screen appears.

Linux Migration - Backup Results screen



Linux Migration - Backup Results

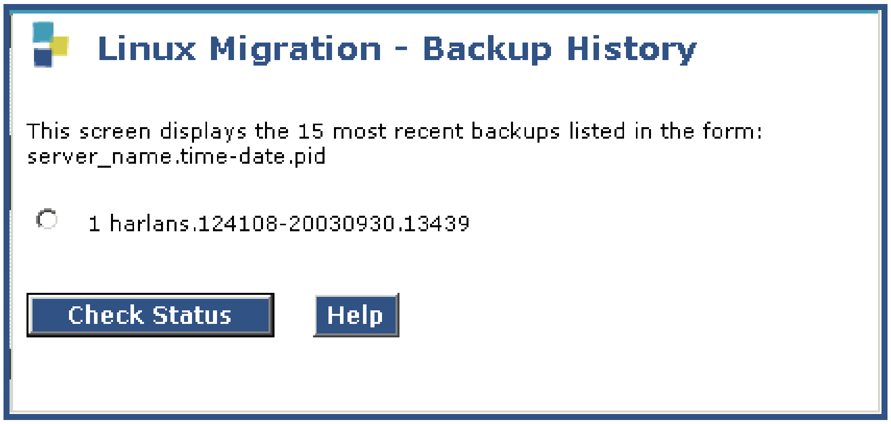
The backup has started. For backup results, click "Status". Select the most recent backup and click "Check Status".

5. Click **Status** to see the backup progress.

Note:

The Linux Migration backup status function is not enabled for release 1.3.1. To check the backup status when upgrading from 1.3.1, select **Backup Status** under **Data Backup/Restore** in the Maintenance Web Interface menu. The **Linux Migration - Backup History** screen appears. Select the appropriate backup set and click **Check Status**.

Linux Migration - Backup History screen



Linux Migration - Backup History

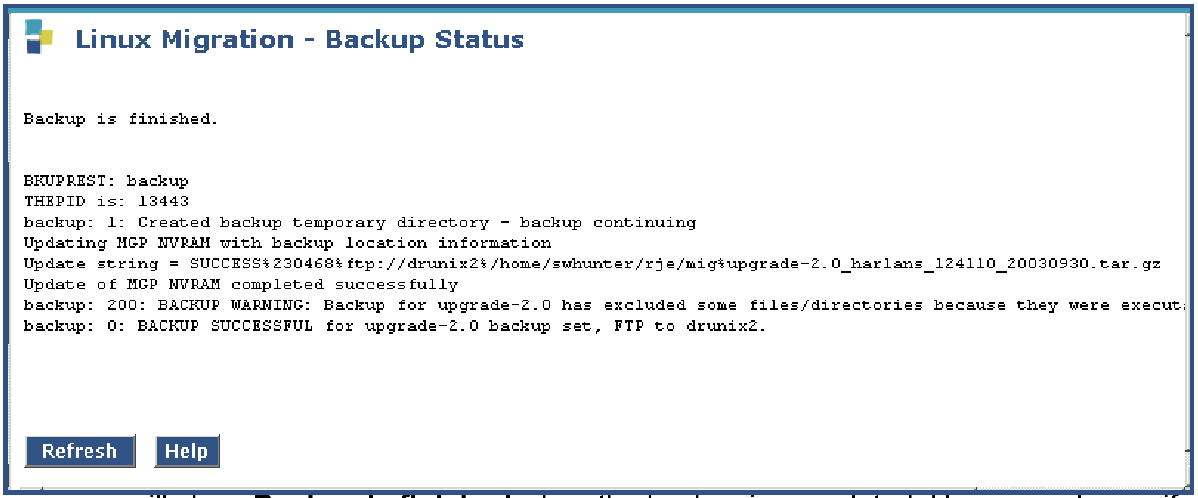
This screen displays the 15 most recent backups listed in the form:
server_name.time-date.pid

○ 1 harlans.124108-20030930.13439

6. Select the backup set and click **Check Status** to see the backup results.

   If the backup is in progress, click **Refresh** until the **Backup is finished** message appears.

Linux Migration - Backup Status screen



Linux Migration - Backup Status

```
Backup is finished.


BKUPREST: backup
THEPID is: 13443
backup: 1: Created backup temporary directory - backup continuing
Updating MGP NVRAM with backup location information
Update string = SUCCESS%230468%ftp://drunix2%/home/swhunter/rje/mig%upgrade-2.0_harlans_124110_20030930.tar.gz
Update of MGP NVRAM completed successfully
backup: 200: BACKUP WARNING: Backup for upgrade-2.0 has excluded some files/directories because they were execut
backup: 0: BACKUP SUCCESSFUL for upgrade-2.0 backup set, FTP to drunix2.
```

The screen will show **Backup is finished** when the backup is completed. However, also verify that the message **Backup Successful** appears in the last line. If any error messages appear stating that the backup failed, follow the normal escalation procedures.

Backing up the system to compact flash media

An S8300C Server with Communication Manager release 4.0 or higher allows back up using a compact flash card. An S8300D Server allows back up using a compact flash card.

To back up the system to compact flash media

1. Plug the cable to the compact flash drive into a USB port on the S8300C Server.
2. Insert a 128-Mb compact flash media into the card reader or writer.

3. On the Maintenance Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.

4. In the Data Sets section select all of the following data sets:

   - If the S8300A/B/C Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - If Communication Manager Messaging is installed on the S8300A or S8300B or S8300C Server, select **Audix**. Also select **Translations, Names and Messages**.

   Note:

   Depending on the customer's Communication Manager Messaging configuration, the back up size of the Communication Manager Messaging data set (**Translations, Names and Messages)** can be larger than the size of the compact flash drive (maximum size of the compact flash drive is 128 MB).

5. Select the Backup Method:

   - Local PC Card

   Tip:

   Backing up to the USB Compact Flash saves time when you are restore data to the migrated server.

6. Optionally, select **Format Compact Flash** to format a new card.

   Note:

   The compact flash card needs to be formatted only before the first use.

7. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

Backing up the system over the customer's LAN

To back up the data on the S8300A, S8300B, or S8300C Server:

1. On the Maintenance Web page, select **Data Backup / Restore > Backup Now**.

   The system displays the **Backup Now** screen.

2. In the **Data Sets** section select all of the following data sets:

   - If the S8300A, S8300B, or S8300C Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**

  - If Communication Manager Messaging is installed on the S8300A or S8300B or S8300C Server, select **Audix**. Also select **Translations, Names and Messages**.

3. Select the Backup Method:
   - Network Device: enter the customer-supplied information for:
     - User Name

       You must enter a valid user name to enable the S8300 Server to log in to the FTP, SFTP, or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.
     - Password

       You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.
     - Host Name

       Enter the DNS name or IP address of the FTP, SFTP, or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).
     - Directory

       Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. If you do not want to use the default directory, you must enter the full path from the ftp server root.
4. Click **Start Backup**.

   Wait for the message indicating that the backup was successful.
5. To check the status of the backup:
   a. Under **Data Backup/Restore**, click **Backup History**.

   b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

      When the backup is finished, the **Backup History Results** screen displays the following message:

   ```
   The final status for your backup job is shown below
   ```

   For each backup set, the following message is displayed if set was backed up successfully:

   ```
   BACKUP SUCCESSFUL
   ```

   ⚠ **Important:**
   When you do full back up, Communication Manager Messaging data is not backed up.

6. If Communication Manager Messaging is installed on the S8300A/B/C, back up announcements:
   - Return to the **Backup Now** screen and uncheck all but **Announcements**.
   - Select the Backup Method (see Step 3 above).
   - Click **Start Backup**.

Recording configuration information

If you have not already done so, you must record the current server configuration data, which must be configured on the new S8300C/D Server.

To view and record the current configuration data

1. Launch the Communication Manager System Management Interface, under the **Administration** menu, click **Server (Maintenance)**.
2. Under **Server Configuration** > click **Configure Server**.
3. Click **Continue** on the first and second screen.
4. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
5. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
6. Select **Configure Interfaces** and record the following:
   - Server IP address
   - Gateway IP address
   - Subnet mask
   - Integrated Messaging IP address, if configured

   You can skip the remaining configuration screens.
7. Select **Close window** and exit the Web pages.

Replacing an S8300-Series Server

The procedure is applicable when you are:

- Replacing S8300A or S8300B Server with an S8300C Server
- Replacing S8300A or S8300B or S8300C Server with an S8300D Server

To remove the old S8300 Server and insert the new S8300 Server

Note:

None of the media gateways in which an S8300A or S8300B or S8300C Server need to be powered down to remove server.

1. On the Maintenance Web page, under **Server**, select **Shutdown Server**.

   Alternatively, you can press the Shutdown button on the server.
2. Select the **Delayed Shutdown** option and clear the **Restart server after shutdown** checkbox.
3. Click the **Shutdown** button.
4. Click **OK** to confirm.
5. When the **OK to Remove** LED on the S8300 faceplate goes on steady, it is safe to remove the S8300 Server.

   ⚠ **CAUTION:**

   Be sure to wear a properly grounded ESD wrist strap when handling the S8300 Server. Place all components on a grounded, static-free surface when working on them.
6. Loosen the two thumb screws on the S8300 faceplate.
7. When removing the S8300A or S8300B Server, remove the LED module (above slot V1) (G700 only) or the space bar (G250, G350) with the S8300 Server.
   - (G700 only) Disengage the LED module and the S8300 Server and remove them together from the gateway.
   - (G250, G350) Remove the space bar and the S8300 Server and remove them together from the gateway.
8. If the Communication Manager Messaging module (CWY1 card) is installed on the S8300B Server, leave it on the S8300B Server.

   Note:

   The CWY1 card is *not* supported on Communication Manager Release 5.2.
9. (G700 only) Reinsert the LED panel (above slot V1) until the front of the panel aligns with the front of the media gateway.

   Note:

   If the LED panel is not inserted all the way in, all of the status lights (on the left side of the LED panel) will be on. If this is the case, press the LED panel all the way in.

10. Connect the DVD/CD-ROM drive with the following steps:

    Note:

    You must do this *before* you completely seat the S8300 Server in the slot.

    a. Connect the USB cable into one of the USB ports on the faceplate of the S8300 Server.

    b. Connect the other end of the USB cable to the CD-ROM or DVD/CD-RW drive.

    c. If you are using an Addonics DVD/CD-RW drive, connect the power cord to the drive and an electrical outlet.

    Note:

    The TEAC drive and S8300 DVD/CD-RW drive get their power from the server over the USB connection.

    d. If you are using the Addonics DVD drive, set the power source switch on the side to **EXT**, *not* **USB**.

    e. If you are using the S8300 DVD/CD-RW drive, set the On/Off switch to **On**.

    Be sure to set the S8300 DVD/CD-RW drive to **Off** when not in use.

11. Insert the Communication Manager Software CD-ROM into the external CD/DVD-ROM drive.

    ⚠ **CAUTION:**

    Verify AC power connection to the laptop. Do not attempt to remaster the S8300 using only the laptop's battery power.

    Note:

    Do not plug any external Compact Flash drive that might be connected to the S8300 C or S8300D Server's USB ports except for the CD/DVD-ROM drive till the installation is complete. The S8300 Server tries to read any media connected to a USB port. The S8300 Server should only read the media on the CD-RW/DVD drive.

12. Insert the S8300C or S8300D Server's into the slot V1 (G700 only) guides or the space bar (G250, G350) until the front of the circuit pack aligns with the front of the media gateway.

    When the server starts to boot, it looks for the software on the DVD/CD-ROM and continues to boot. The Alarm LED of the S8300 Server lights steadily as it is starting. The Alarm LED starts flashing when the S8300 Server is ready to load software.

13. Secure the S8300C or S8300D Server's faceplate with the thumb screws.

    Tighten the thumb screws with a screw driver.

14. Reconnect the laptop to the services port of the new S8300C or S8300D Server.‘

Installing Communication Manager Release 5.2 (Optionally, Communication Manager Messaging)

To install Communication Manager release 5.2 (Optionally Communication Manager Messaging on the server):

1. On your laptop click **Start > Run** to open the **Run** dialog box.
2. Type **ping -t** `192.11.13.6` and press **Enter**. Wait for the reply.
3. The installation script looks for the software CD in the CD/DVD drive connected to the USB port. If the CD/DVD drive was not attached to a USB port when the server booted up, you see **Request Timed Out** on the screen. In this case unseat and reseat the S8300C or S8300D in its slot.

   Tip:

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

4. Select **Install** and press **Enter**.

   The **Select Release Version** screen appears.

5. Select the appropriate release version then select **OK** and press **Enter**.

   The **Run Communication Manager Messaging Installation** screen appears.

Note:

The Communication Manager Messaging is optionally installed on the server when you install Communication Manager. If the customer was not using Communication Manager Messaging before migration, the customer can can optionally install Communication Manager Messaging on the S8300C or S8300D Server.

6. Select **Yes** if you want to install Communication Manager Messaging concurrently with Communication Manager; select **No** if you do not.

   The following processes are initiated:

   - The server's hard drive and internal Compact Flash are partitioned and reformatted.
   - The Linux operating system is installed.
   - Communication Manager software is installed and the progress reported.
   - If selected, Communication Manager Messaging is installed.

   The process takes about 30 minutes. When the server is ready to reboot, the CD drive door opens and a reminder to check the Avaya Support Site (http://support.avaya.com/downloads) for the latest software and firmware updates appears.

   The reboot takes 1-3 minutes without Communication Manager Messaging and 3-6 minutes with Communication Manager Messaging.

7. On your laptop, click **Start > Run** to open the **Run** dialog box.
8. Type `ping -t 192.11.13.6` and press **Enter**.
9. Wait for the reply from the server to ensure connectivity to it.

For the remaining steps on installing Communication Manager and co-resident applications, please refer the *Installing and Configuring the Avaya S8300 Server*, 555-234-100 guide .

To check reboot progress

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

   This command will have one of the following results:

   - 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.
4. Type ping -t 192.11.13.6 to access the media server.

   The -t causes the ping to repeat until you get a response. When you get a response (in about 3 minutes), wait an additional 30 seconds before going back to the Web interface.
5. Type ctrl c to stop the ping.
6. Close the MS-DOS window.To check reboot progress

Verifying the software version

Note:

Since the system is now running a new software release, you must login with the ***initial craft ID and password***. (You cannot use ***dadmin*** at this point.)

To verify the software version that you just installed:

1. Visit, https://192.11.13.6.
2. Click **Server (Maintenance)** from the **Administration** menu.
3. Select **Server > Software Version**.
4. The **Software Version** page appears.
5. Verify that the server is running Release 5.2 software. The beginning of the **Report as:** string should show **R015x.02**.
6. Verify that the DVD/CD-ROM drive opened at the end of the software installation.

7. Disconnect the DVD/CD-ROM drive from the server's USB port.

Setting the time, date, and time zone

To set the time, date, and time zone on the server:

1. On the System Management Interface page, select **Server > Server Date/Time**.

   The **Server Date/Time** window displays.

2. Set the server time within five (5) minutes of the Network Timer Server (NTS) time, date and time zone so that synchronization can occur.

   ⚠ **Important:**
   If you change the time zone, you must reboot the server.

Copying files to the S8300 Server

While reformatting the hard drive a new directory, */var/home/ftp/pub*, was created. You must copy the following files to the *pub* directory on the server's hard drive:

- Communication Manager software service pack
- License file
- Avaya authentication file
- Updated media gateway, media modules, or IP telephony firmware files
- Security updates
- Messaging application service packs, RFUs, announcement files, or language sets

To copy files to the server:

1. On the System Management Interface, click **Server (Maintenance)** under the **Administration** menu.
2. Select **Miscellaneous > Download Files**.

   The **Download Files** page appears.

3. Select **File(s) to download from the machine I'm using to connect to the server**.
4. Click **Browse** to open the **Choose File** window to navigate to the files you want to download.
5. Select the file(s) to download.

Note:

If you need to download an IP telephone firmware file, download this file last with **Install this file on the local server** checked. The files are copied to the /tftpboot directory, the IP telephone Web page is reinstated, and the firmware is restored at the next reboot.

Note:

To manually FTP files from your laptop to */var/home/ftp/pub*, you must change the directory to *pub* (type **`cd pub`**) after starting FTP and logging in.

6. Click **Download** to copy the files to the server.

   The transfer is complete when the following message appears:

   ```
   Files have been successfully downloaded to the server
   ```

⚠ **Important:**

Remove the Communication Manager software distribution CD from the DVD/CD-ROM drive.

Downloading optional language files

If the optional language files are needed, copy the files from the language CD to */var/home/ftp/pub*.

1. Insert the language CD in your laptop's CD-ROM drive.
2. At the Maintenance Web Pages, select **Miscellaneous > Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.
4. Browse to the laptop CD and select each language file that you want to copy to the server.
5. Click **Download**.

   The transfer is complete when the following message appears:

   ```
   Files have been successfully downloaded to the server
   ```

6. If you need to copy more than four (4) optional language files, repeat this procedure.

   Copies of the optional language files are now in the */var/home/ftp/pub* directory and are automatically installed during the next reboot.

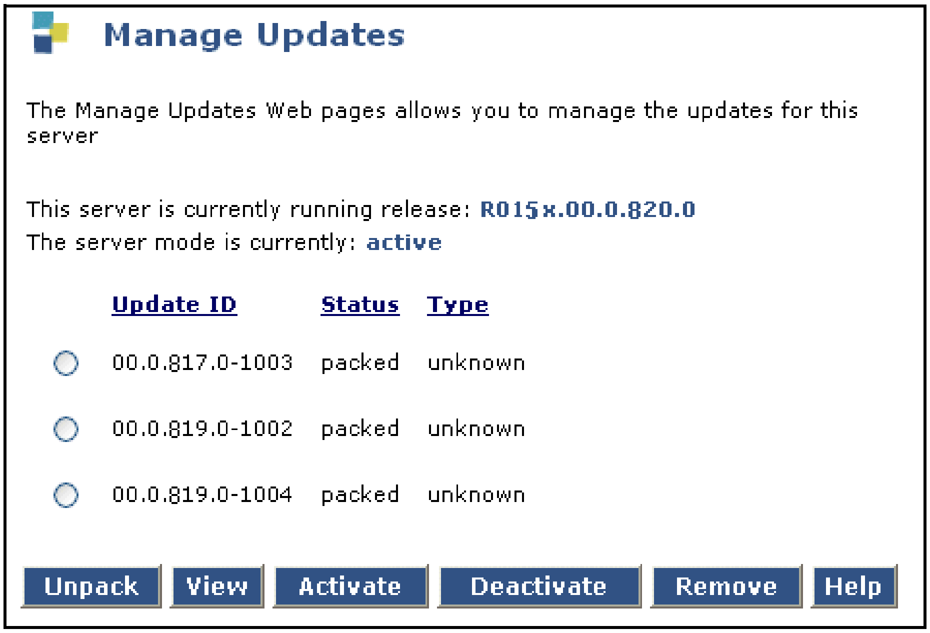
Installing security updates, Communication Manager service pack updates, and SES service pack updates, if any

To install update files

1. Under Server Upgrades, select **Manage Updates**.

   The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allows you to manage the updates for this server

This server is currently running release: R015x.00.0.820.0

The server mode is currently: active

	Update ID	Status	Type
○	00.0.817.0-1003	packed	unknown
○	00.0.819.0-1002	packed	unknown
○	00.0.819.0-1004	packed	unknown

2. If an update file you want to activate shows **packed** in the **Status** column, select the file in the **Update ID** column, and click **Unpack**.

   The window shows the status of the unpacking.

3. Wait until the system displays the message `...unpacked successfully` and click **Continue**.

   The system displays the **Manage Updates** screen.

4. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

   The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

5. Click **Yes**.

   Wait until the system displays the Continue button.

6. Click **Continue**.

Enable SES

Note:

Perform this task if the migration is from S8300C to S8300D and if SES was enabled on the S8300C. Skip this task if the S8300 is an LSP.

To enable SES:

1. On the **Server (Maintenance)** Web page select **Miscellaneous > SES Software**.

   The **SES Software** page displays, and the text, "SES is disabled" should appear just above the Enable SES button.

2. Click **Enable SES**.
3. Wait approximately 30 seconds and click the refresh button on your browser.

   The **SES Software** page should show, "SES is enabled."

4. To verify that SES is enabled go to the **Communication Manager System Management Interface** main page.
5. Verify that the **SES Administration** is on the **Administration** menu.

Configuring network parameters

Note:

You must have the host name, subnet mask, and IP addresses of the server and default gateway to complete this procedure.

⚠ **Important:**

You must configure the network parameters on the S8300 before restoring the backup files.

To configure the network parameters on the server:

1. On the System Management Interface, click **Configure Server** under the **Installation** menu.

   The **Configure Server** wizard launches.

2. Click **Continue** until you get to the "Specify how you want to use this wizard" screen.
3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the "Configure Individual IP Services" list on the left.

   The **Set Identities** page appears.

5. Fill in the host name with the name of the server.

6. Click **Continue**.

   The **Configure Interfaces** page appears.

7. Fill in the correct server and gateway IP addresses, the subnet mask, and, if CM Messaging is installed, its IP address (but not if this server is an LSP).

   If these fields are already filled in, overwrite them with the correct information. Leave the **Integrated Message** field blank.

8. Click **Change** to update the system files.

   Note:

   If an Action Cancelled message appears before the Success message, refresh the screen and click **Change** again.

9. When the configuration change is complete, the "Successfully configured ethernet interfaces" message appears.

Verifying connectivity

To verify that the Ethernet port is working, ping the FTP server where the backup file(s) are stored.

1. On the **Server (Maintenance)** Web page, select **Diagnostics > Ping**.
2. Enter the IP address of the device on which the backup files are stored.
3. Click **Execute Ping**.

   If the ping is successful, continue with Restoring backup data. Otherwise, check the IP address and connectivity to the server.

Restoring backup data

To restore backup data:

1. Select **Data Backup/Restore > View/Restore Data**.

   The **View/Restore Data** page appears.

2. Select **Network Device**.
3. In the **Method** drop-down box, select **FTP**.
4. Fill in these fields:
   - **User Name**
   - **Password**
   - **Host Name** (enter the host IP address)

- **Directory**

5. Click **View**.

   The **View/Restore Data Results** page appears.

6. If you need to restore the OS data set (server and system files), restore the OS data set first. If not, restore the security data set now.

7. Select both "Force..." options then click **Restore**.

8. To monitor the restore progress at the Maintenance Web Pages, select **Data Backup/ Restore > Restore History**.

   The **Restore History** page appears.

9. Select the backup file that you want to monitor and click **Check Status**.

   The **Restore History Results** page appears.

10. Click **Refresh** periodically until the message indicates that the restore was successful. This takes approximately five (5) minutes.

11. Repeat Steps 1-10 above to restore:

    a. Security data set (if not performed in Step 6 above).

    b. Communication Manager translations (main server/primary controller only, not an LSP) data.

    c. Messaging application data in the "audix-tr-name-msg" file (primary controller only, not an LSP).

    d. Messaging application announcements in the "audix-ann" file (primary controller only, not an LSP).

Checking for a super-user login

Note:

> If you restored Communication Manager translations (xln file) earlier, omit this section and continue with Installing updated Communication Manager license and authentication files on page 386.

When you are replacing a server or hard drive, the Communication Manager Maintenance Web Pages might time out if too much times elapses without activity. In this case, you might not be able to log in again with the *craft* login. This problem can occur after you install the new server and restore translation and security files, but *before* you install the new authentication file. Restoring translation and security files does not restore the *init* and *inads* service accounts, nor is "sroot" available until the authentication file is installed. However, you *can* log in with the customer’s super-user login, if it exists.

To ensure that a super-user login exists in Communication Manager:

1. SSH to and log in as *craft* to the server command line interface.

2. At the Linux command line interface type **`cat /etc/passwd |grep 555`** and press **Enter**.

   A list of super-user logins displays (example only):

   ```
   init:x:778:555::/var/home/defty:/bin/bash
   inads:x:779:555::/var/home/defty:/bin/bash
   craft:x:780:555::/var/home/defty:/bin/bash
   dadmin:x:1101:555::/var/home/defty:/bin/bash
   erik:s:1002:555::/var/home/defty:/bin/bash
   ```

   Look for any logins other than the *init*, *inads*, and *craft* logins. If no additional super-user logins exist, you must create one (Creating a super-user login on page 383).

Creating a super-user login

Note:

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

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

Use the **Integrated Management Maintenance Web Pages** to create a super-user login.

To create a login:

Note:

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

1. In the **Integrated Management Maintenance Web Pages**, under **Security**, select **Administrator Accounts**.
2. Select **Add Login**.
3. Select **Privileged Administrator** and click **Submit**.

   The **Administrator Accounts -- Add Login: Privileged Administrator** screen appears.
4. Type a login name for the account in the **Login name** field.
5. Verify the following:

   - **susers** appears in the **Primary group** field.
   - **prof18** appears in the **Additional groups (profile)** field. *prof18* is the code for the customer superuser.
   - **/bin/bash** appears in the **Linux shell** field.
   - **/var/home/*login name*** appears in the **Home directory** field, where ***login name*** is the name you entered in step 4.

6. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
7. For the **Select type of authentication** option, select **password**.

Note:

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

8. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
9. In the section **Force password/key change on next login** select **no**.
10. Click **Submit**.

    The system informs you the login is added successfully.

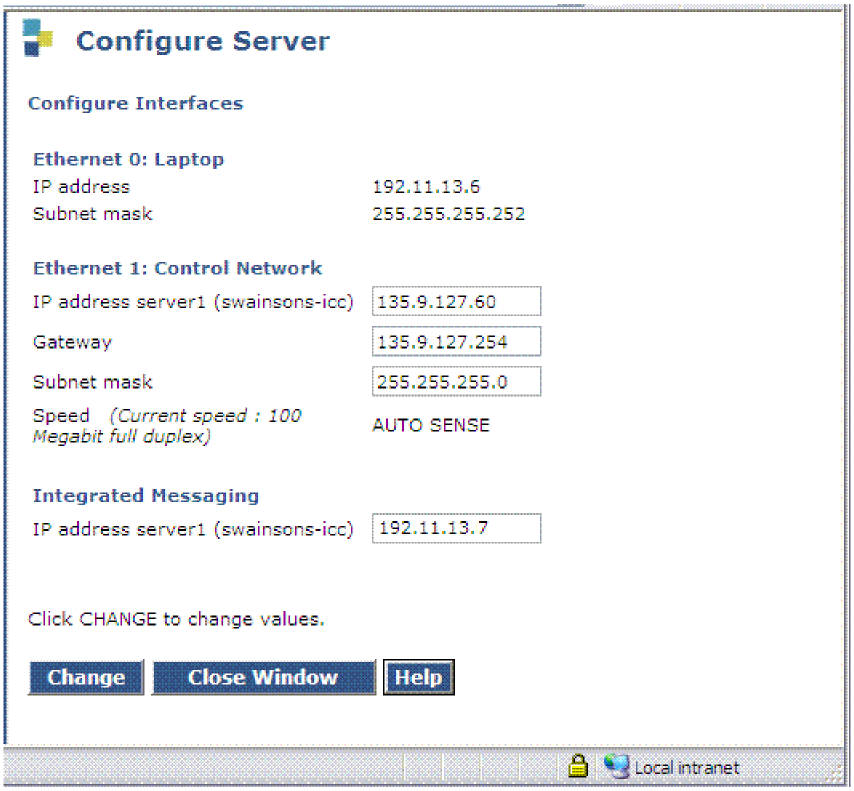
Checking for the CM Messaging IP address

To check the CM Messaging IP:

1. On the System Management Interface Web page, click **Configure Server** under the **Installation** menu.
2. Click **Continue** through the **Review and Backup Notices** to get to the **Specify how you want to use this wizard** screen.
3. Click **Configure Interfaces** from the “Configure Individual IP Services” list on the left.

The **Configure Interfaces** screen appears.

Configure Interfaces screen (primary controller example)



Configure Server

Configure Interfaces

Ethernet 0: Laptop

IP address 192.11.13.6

Subnet mask 255.255.255.252

Ethernet 1: Control Network

IP address server1 (swainsons-icc) 135.9.127.60

Gateway 135.9.127.254

Subnet mask 255.255.255.0

Speed *(Current speed : 100 Megabit full duplex)* AUTO SENSE

Integrated Messaging

IP address server1 (swainsons-icc) 192.11.13.7

Click CHANGE to change values.

4. Check that the Integrated Messaging IP address is available:
   - If the IP address is available, click **Close Window**.
   - If the IP address is not available, enter the IP address and click **Change**.

Note:

> If an Action Cancelled message appears before the Success message, refresh the screen and click **Change** again.

When the configuration change is complete, the screen displays the following message: `Successfully configured ethernet interfaces`. Click **Close Window**.

At this point, the system resets the IP interfaces.

Installing updated Communication Manager license and authentication files

CAUTION:

A super-user login, dadmin, or other customer super-user login must exist *before* you install an authentication file. See Creating a super-user login on page 383.

To install the Communication Manager license and authentication files:

1. On the **Server (Maintenance)** Web page, select **Security > License File**.

   The **License File** page appears.

2. Select **Install the license file I previously downloaded** and click **Submit**.

   The system displays a message telling you that the license was installed successfully.

3. At the Maintenance Web Pages, select **Security > Authentication File**.

   The **Authentication File** page appears.

4. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system displays a message telling you that the authentication file was installed successfully.

5. Verify the license and authentication file installation by typing the `statuslicense -v` command from the server command line:

   - The **License Mode** should be **Normal**.
   - The report should list a **License Serial Number**.

Installing the SES license

If you enabled SES on the **Server (Maintenance)** Web page, you must install the SES license from the WebLM server that is located on an edge or a combined home/edge server:

1. On the **System Management Interface** Web page, under the **Installation** menu, click **SIP Enablement Services**.

   The system displays the **Integrated Management SIP Server Management** screen.

2. Select **Server Configuration > License**.

   The **List Licenses** page displays.

3. Click **Access WebLM**.

   The **WebLM** application screen displays in a new window.

4. If this is the first time the application has run, you must log in with *admin* as the default login and *weblmadmin* as the default password, then change both the default login and password to the customer's preferences for this account.

   Note:

   > If the WebLM server is on a different subnet than the server, you must change the URL in your browser to include the server's DNS name. When you mouse-over the WebLM link on the List Licenses page, the URL includes an IP address, for example, "https://12.34.56.78/WebLM/index.jsp/." Change the URL to "https://*server-name*/WebLM/index.jsp/," where *server-name* is the DNS name of the server on which you want to install the SES license.

5. Select **License Administration**.

   The authentication screen appears.

6. Login as *admin* and enter the password.

   After this initial login, the system prompts you to change the password.

7. Change the password.

   WebLM logs you out.

8. Log in again as *admin* with the newly-created password.

   The **Web License Manager (WebLM)** screen appears.

9. Select **Install License**.

   The **Install License** page displays.

10. Click **Browse** to navigate to the SES license that you want to install.

11. Click **Install**.

    If the license is valid, the system indicates that it was installed successfully; otherwise the process fails with a brief description.

    Note:

    > The license update for the home seats can take up to 15 minutes. Wait approximately 15 minutes before continuing with verifying the license installation (Step 12).

12. To verify the license installation go to the Integrated Management SIP Server Management **Top** page and select **Server Configuration > License**.

    The **List Licenses** page displays.

13. Ensure that the following three (3) licenses are listed in the **Name** column:

    - Edge Proxy
    - Basic Proxy
    - Home Seats

14. Click **Show** by the Edge Proxy listing.

    The **License Information** page displays.

15. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   1
    Acquired    1
    ```

16. Click **Show** by the Basic Proxy listing.

    The **License Information** page displays.

17. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   1
    Acquired    1
    ```

18. Click **Show** by the Home Seats listing.

    The **License Information** page displays.

19. Ensure that the page displays the following information:

    ```
    Proxy Name  sipserver
    Requested   XXX
    Acquired    XXX
    ```

    where `XXX` is the actual number of seats in the license.

20. Reboot the S8300 server:

    a. Click **Shutdown Server** under the Server heading.

    b. Select **Delayed Shutdown and Restart server after shutdown**.

    c. Click **Shutdown**.

    You will be logged off the server when it reboots. You can use ping to verify when the server is accessible again.

Rebooting the server

To instate the foregoing administration and provisioning:

1. On the **Server (Maintenance)** Web page, select **Server > Shutdown** server.

   The **Shutdown This Server** page appears.

2. Select **Delayed Shutdown** and check the **Restart server after shutdown** box.

3. Click **Shutdown**.

Integrity check

After the server comes up, verify the following:

1. Ping the IP address of the server and ensure connectivity.
2. On the **Server (Maintenance)** Web page, select **Server > Status Summary**.

   The **Status Summary** page appears.
3. Verify the following:
   - **Mode** is **Active**.
   - **Server Hardware** is **okay**.
   - **Processes** is **okay**.
4. At the Maintenance Web Pages, select **Server > Process Status**.

   The **Process Status** page appears.
5. In the Content section, select **Summary**.
6. In the Frequency section, select **Display once**.
7. Click **View**.

   The **View Process Status Results** page appears.
8. Verify that all processes are **UP**.

If CM Messaging is installed

Complete this section only if CM Messaging is installed. Otherwise continue with If the S8300 is an LSP on page 391.

Verify the CM Messaging address

If the CM Messaging is installed, verify its IP address:

1. Select **Server Configuration > Configure Server**.

   The **Configure Server** wizard launches.
2. Click the **Continue** button until you get to the **Specify how you want to use this wizard** screen.

   The **Configure Interfaces** screen appears.
3. Check that the **Integrated Messaging IP address** appears:

- If the IP address appears, click **Close Window**.
- If the IP address does not appear, enter the IP address and click **Change**.

Note:

If an Action Cancelled message appears before the Success message, refresh the screen and click **Change** again.

4. When the configuration change is complete the following message is displayed:`Successfully configured ethernet interfaces`. Click **Close Window**.

   The system resets the IP interfaces.

Verify that CM Messaging has started

Note:

The Communication Manager license must be installed before you can verify whether CM Messaging has started.

To verify that the CM Messaging has started:

1. Select **Server > Process Status**.
2. Select **Summary and Display once** and click **View**.

   The **View Process Status Results** page appears.
3. Ensure that **Messaging** is **UP**.

   If Messaging is not **UP** you can start it either of two ways:

   - **Messaging Web Pages**

     a. At the Maintenance Web Pages, select **Miscellaneous > Messaging Software**.

        The **Messaging Software** page displays "Internal messaging is disabled."

     b. Click **Enable**.

        The **Messaging Software** page is updated with an "execution successful..." message at the top of the page and another indicating "Internal messaging is enabled."

   - **Server command line**

     a. Access the server’s command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

     b. Type **`start -s Audix`** and press **Enter**.

     c. Verify that all Communication Manager processes come up.

     d. Monitor the CM Messaging startup with the **`watch /VM/bin/ss`** command.

        The display periodically refreshes automatically.

     e. When CM Messaging is up, type **Ctrl+C** to end the **`watch`** command.

If the S8300 is an LSP

Perform this procedure if the server if all of the following are true:

- Server is an S8300C or S8300D
- Server is an LSP and the primary controller for this LSP is or will be an S8720 configured as XL, or an S8730 Server

Note:

Skip this procedure and go to Save translations (on main server only) on page 393, if one or more of the following are true:

- Server is a primary controller (S8300B/C/D as a primary controller cannot be configured as Extra Large memory configuration).
- Server is an S8300B LSP (S8300B LSP cannot be configured to be compatible with S8720 XL or S8730)
- Server is an LSP and is already configured to be compatible to XL (the restore of full or os datasets will retain the setting from the server that was backed up).

If upgrading an S8300C LSP, configuring the LSP for compatibility with an XL configuration

Note:

If the primary controller is an S8720 or S8730 configured as XL, the LSP must be an S8300C and must be configured as XL. The S8300B cannot be an LSP for a primary server configured as XL.

To configure the S8300C LSP to be compatible with the *main* S8720 in XL configuration or the *main* S8730 Server:

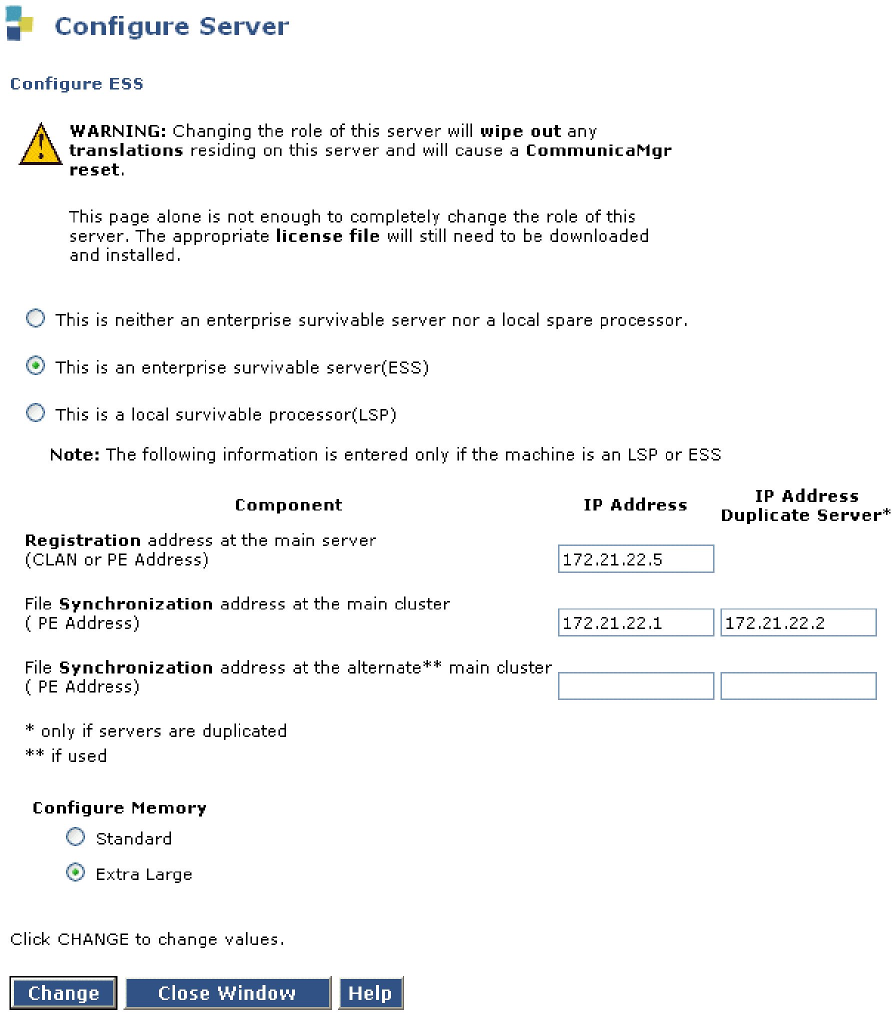
1. At the server command line interface, type `stop -acfn` and press **Enter** to stop Communication Manager call processing.
2. On the System Management Interface Web page, click **Configure Server** under the **Installation** menu.

   The system displays the **Review Notices** screen.
3. Click **Continue** until you get to the **Specify how you want to use this wizard** screen.

   ⚠ **CAUTION:**

   For the next step, if you select and save as **Extra Large** you cannot revert to **Standard**. If you try to go back to **Standard**, server translation corruption occurs.
4. Select **Configure individual services** and click **Continue**.

5. In the left column, click **Configure LSP**.



Configure Server

Configure ESS

WARNING: Changing the role of this server will **wipe out** any **translations** residing on this server and will cause a **CommunicaMgr reset**.

This page alone is not enough to completely change the role of this server. The appropriate **license file** will still need to be downloaded and installed.

○ This is neither an enterprise survivable server nor a local spare processor.

● This is an enterprise survivable server(ESS)

○ This is a local survivable processor(LSP)

Note: The following information is entered only if the machine is an LSP or ESS

Component	IP Address	IP Address Duplicate Server*
Registration address at the main server (CLAN or PE Address)	172.21.22.5	
File **Synchronization** address at the main cluster (PE Address)	172.21.22.1	172.21.22.2
File **Synchronization** address at the alternate** main cluster (PE Address)		

* only if servers are duplicated
** if used

Configure Memory

○ Standard

● Extra Large

Click CHANGE to change values.

6. Select **Extra Large** and click **Change**.
7. Click **Close Window**.
8. At the server command line interface, type `start -ac` and press **Enter** to restart Communication Manager call processing.
9. At the server command line interface, type `swversion` and press **Enter**.
10. In the **Memory Config** field, verify that the setting is **Extra Large**.

If upgrading an LSP, synchronize translations from the primary controller

If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

1. Log in to the SAT with **`telnet`** or **`ssh`**.
2. At the SAT prompt, type **`save translation lsp`** and press **Enter**.

   Under **Command Completion Status** you should see `Success`.

Save translations (on main server only)

To synchronize the main server's translations with the LSP:

1. Log in to the main server's SAT interface.
2. At the SAT prompt type **`save translation lsp`** and press **Enter**.

   Look for "Success" in the Command Completion Status section.
3. Logoff the system.
4. Release alarm suppression when prompted.

   Note:

   The time that it takes to synchronize the files with the LSP depends on the system and network resources.
5. Verify that the translations have synchronized with the LSP at the main server's SAT interface by typing **`list survivable-processor`** and press **Enter**.
6. Verify that this LSP server is listed and registered. Look for "Y" in the **Reg**(istered) column.

Copying IP Phone firmware to the server, if necessary

If, before the upgrade, the server was serving as an http server for IP phone firmware, download the most recent IP phone firmware bundle available from the Avaya Firmware Download Web site. The firmware bundle reinstates the 46xx IP Phone Web page in Communication Manager and also makes the 46xx IP Phone firmware for the tftp or http server capability of the server.

Note:

The IP phone firmware that was originally downloaded will have been overwritten.

To copy files to the server:

1. In the Maintenance Web Interface, under **Miscellaneous**, select **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server.**
3. Click **Browse** next to the top field to open the **Choose File** window on your computer. Find the files that you need to copy to the server.
4. Click **Install this file on the local server**.
5. Click **Download** to copy the file(s) to the server.

   The files are copied automatically to the /tftpboot directory. The 46xx IP Phone Web page is reinstated at the next reboot.

Installing IP phone firmware download configuration file

If the S8300B was running 3.1.3 (R013x.01.3.640.2) or later software and you used the restore of either the **os** data set or the **full** data set to configure the S8300C Server, skip this procedure.

Perform this procedure if the S8300C Server is being used to support firmware downloads to IP telephones, and the S8300B Server was running 3.1.2 (R013.01.2.632.1) or earlier release of software.

Use the following steps to restore the 46xxsettings.txt file to the S8300 Server:

1. Use FTP or SFTP to move the 46xxsettings.txt file to the S8300 Server. The file is transferred to the */var/home/ftp/pub* directory.
2. At the server command line interface, type **`cp /var/home/ftp/pub/46xxsettings.txt /tftpboot`**.

If CM Messaging fails to start after an upgrade

If you have upgraded your Communication Manager and CM Messaging software, you must have a new license that is associated with the latest release. CM Messaging will not use the license for a previous version.

If you upgraded CM Messaging without a new license file, it will fail to start during the Communication Manager startup sequence.

If this occurs, you must perform the following steps:

1. Obtain an CM Messaging license file.
2. Install the license file.
3. From a command prompt, start the CM Messaging process with the following command:

   ```
   start -s Audix
   ```

Post-upgrade tasks

Stopping CM Messaging, if loading an CM Messaging update

After the upgrade is complete, perform the following post-upgrade tasks.

1. Click **Messaging** from the **Administration** menu.

   The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, under **Utilities**, select **Stop Messaging**.

   The **Stop Messaging Software** Web page is displayed.

3. Select the **Stop** button.

   The shutdown of the messaging server will begin when all users have logged off from CM Messaging or after three minutes have passed, whichever event comes first. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing CM Messaging service pack (or RFU) files, if any

If CM Messaging is being used, a post-upgrade service pack for CM Messaging may be required. See the CM Messaging documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at http://support.avaya.com.

1. Under **Software Management,** select **Adv Software Installation**.
2. Select **Continue this operation without current system backup**.
3. Select the CM Messaging update package and click **Install Selected Packages**.

   Note:

   > The system automatically prompts you to restart CM Messaging when the service pack has been installed. Therefore, if you restart CM Messaging at this time, you do *not* need to perform the following procedure, Starting CM Messaging on page 396.

Starting CM Messaging

⚠ **CAUTION:**

You do *not* need to perform this task if you restarted CM Messaging as a part of the installation of the CM Messaging service pack.

After the CM Messaging application has been updated, you must restart it using the following steps:

1. On the **Messaging Administration** Web page, under **Utilities**, select **Start Messaging**.

   The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

2. When the message `End start_vm: voice messaging is now completely up` is displayed, close the Messaging Administration Web page and perform the next procedure in this document.

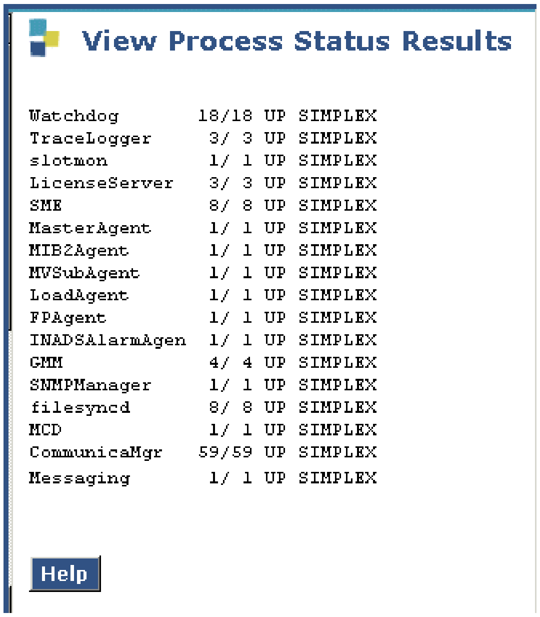
Verifying start up of CM Messaging

To verify operation of CM Messaging, perform the following steps:

1. On the **Server (Maintenance)** Web page, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

   The **View Process Status Results** screen appears.

View Process Status screen



View Process Status Results

```
Watchdog        18/18 UP SIMPLEX
TraceLogger      3/ 3 UP SIMPLEX
slotmon          1/ 1 UP SIMPLEX
LicenseServer    3/ 3 UP SIMPLEX
SME              8/ 8 UP SIMPLEX
MasterAgent      1/ 1 UP SIMPLEX
MIB2Agent        1/ 1 UP SIMPLEX
MVSubAgent       1/ 1 UP SIMPLEX
LoadAgent        1/ 1 UP SIMPLEX
FPAgent          1/ 1 UP SIMPLEX
INADSAlarmAgen   1/ 1 UP SIMPLEX
GMM              4/ 4 UP SIMPLEX
SNMPManager      1/ 1 UP SIMPLEX
filesyncd        8/ 8 UP SIMPLEX
MCD              1/ 1 UP SIMPLEX
CommunicaMgr    59/59 UP SIMPLEX
Messaging        1/ 1 UP SIMPLEX
```

3. Make sure Messaging shows **UP**.

   The number of processes (59/59) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 58/59 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an CM Messaging sanity test:
   a. At the Linux command line, type **`/vs/bin/display`**.
   b. Verify that all states are `Inserv`.
   c. Retrieve the test message saved before the upgrade.
6. At the Linux command line, type **`/VM/bin/ss`**.
7. Verify that all CM Messaging processes are shown.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.

3. Type **`save translation all`** and press **Enter**.

   When the save is finished, the following message appears:

   ```
   Command successfully completed.
   ```

Administering CM Messaging switch integration for H.323, if necessary

The CM Messaging application uses H.323 signaling instead of the CWY1 board for integration with Communication Manager. If the previous release on the S8300 Server used the CWY1 board, you must administer the CM Messaging switch integration for H.323. The tasks for administering the H.323 integration are explained in *Administering Servers to work with IA770*.

Testing to verify system functionality

If you are upgrading an S8300 primary controller, test the system for functionality.

1. Verify the following:
   - Telephones have dial tone
   - You can call from one telephone to another telephone on the system
   - You can make an external trunk call.
   - The media gateways have registered. Use the SAT command **`list media-gateway`**.

Completing the upgrade process (S8300 is the primary controller)

Telnet to the S8300 (primary controller) and open a SAT session:

1. To check media modules on page 399
2. To enable scheduled maintenance on page 399
3. To busy out trunks on page 399
4. To check for translation corruption on page 399
5. To resolve alarms on page 399
6. To re-enable alarm origination on page 400
7. Backing up the S8300A or S8300B or S8300C Server data on page 366

To check media modules

1. Type `list configuration all` and press **Enter**.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that <replace with long product name> is working.

To enable scheduled maintenance

1. Type `change system-parameters maintenance` and press **Enter**.
2. Ensure that the **Start Time** and **Stop Time** fields' administration is the same as before the upgrade.

To busy out trunks

1. Busy out trunks that were busied out before the upgrade (see To busy out trunks on page 349).

To check for translation corruption

1. Type `newterm` and press **Enter**.

   If you do not get a login prompt and the following message appears,

   ```
   Warning: Translation corruption detected
   ```

   follow the normal escalation procedure for translation corruption before continuing the upgrade.

To resolve alarms

1. In the Maintenance Web Interface, under Alarms click **Current Alarms** to examine the alarm log.
2. If any alarms are listed, click **Clear All**.
3. Resolve new alarms that have appeared since the upgrade through <replace with long product name>. For instructions see the appropriate maintenance book.

To re-enable alarm origination

1. Telnet to the S8300 and log on.
2. At the command prompt, type **`almenable -d b -s y`**

   where

   `-d b` sets the dialout option to *both* (numbers)

   `-s y` enables SNMP alarm origination
3. Type **`almenable`** (without any options) to verify alarm origination enabled status.

If CM Messaging fails to start after a new installation

If you have installed or upgraded CM Messaging and it does not start, you must ensure that an IP address has been provided for use with CM Messaging. To check for the IP address, you must use the **Configure Server** option through the Maintenance Web pages.

On the Configure Interfaces screen, ensure that a valid IP address is present in the **Integrated Messaging** section**.**

Backing up the system

To back up the system to compact flash media (S8300C or S8300D Server only)

1. Plug the cable to the compact flash drive into a USB port on the S8300C.
2. Insert a 128-Mb compact flash media into the top right slot of the drive.
3. On the **Server (Maintenance)** Web page, select **Backup Now**.

   The system displays the **Backup Now** screen.
4. In the Data Sets section select all of the following data sets:
   - If the S8300B, S8300C, or S8300D Server is ***not*** an LSP, select **ACP Translations**; select **Save ACP translations before backup**.
   - **Server and System Files**
   - **Security Files**
   - If Communication Manager Messaging is installed on the S8300B, S8300C, or S8300D Server, select **Translations, Names and Messages**.

Note:

Depending on the customer's Communication Manager Messaging configuration, the back up size of the Communication Manager Messaging data set (**Translations, Names and Messages)** can be larger than the size of the compact flash drive (maximum size of the compact flash drive is 128 MB).

5. Select **Local Compact Flash Card** to back up the data onto the compact flash card.

   Optionally, select **Format Compact Flash** to format a new card.

   Note:

   The compact flash card needs to be formatted only before the first use.

6. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

To back up the system over the customer's LAN

1. Make sure you have the IP address of the customer's FTP, SFTP, or SCP backup server.
2. On the S8300 main menu, select **Backup Now**.
3. The system displays the **Backup Now** screen.
4. Select the type of data you want to back up by selecting the appropriate data set.
5. Select the Backup Method, normally **FTP**, **SFTP**, or **SCP**, to indicate the destination to which the system sends the backup data:
   - Network Device: enter the customer-supplied information for:

- **User name**

  You must enter a valid user name to enable the S8300 Server to log in to the FTP, SFTP, or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.

- **Password**

  You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.

- **Host name**

  Enter the DNS name or IP address of the FTP, SFTP, or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

- **Directory**

  Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. If you do not want to use the default directory, you must enter the path name for the directory.

6. Click **Start Backup**.

   The system displays the results of your backup procedure on the **Backup Now** results screen.

7. To check the status of the backup:

   a. Under **Data Backup/Restore**, click **Backup History**.

   b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

      When the backup is finished, the **Backup History Results** screen displays the following message:

   ```
   The final status for your backup job is shown below
   ```

   For each backup set, the following message is displayed if set was backed up successfully:

   ```
   BACKUP SUCCESSFUL
   ```

   ⚠ **Important:**
   When you do full back up, Communication Manager Messaging data is not backed up.

8. If Communication Manager Messaging is installed on the S8300A , S8300B, or S8300C back up announcements:

   - Return to the **Backup Now** screen and uncheck all but **Announcements**.
   - Select the Backup Method (see Step 5 above).
   - Click **Start Backup**.

This completes the installation of the G700 Media Gateway with an S8300 Server as primary controller.

Index