



**Installing and Configuring the  
Avaya S8700-Series Server  
Release 5.0**

03-300145  
Release 5.0  
January 2008  
Issue 7

© 2008 Avaya Inc.  
All Rights Reserved.

#### **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 legal page information, please see the documents, *Avaya Support Notices for Software Documentation*, 03-600758, and *Avaya Support Notices for Hardware Documentation*, 03-600759.

These documents can be accessed on the documentation CD and on the Web site, <http://www.avaya.com/support>. On the Web site, 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**

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.

#### **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

|  |           |
|--|-----------|
| <b>Chapter 1: Introduction</b> . . . . .                                       | <b>7</b>  |
| Audience . . . . .   | 7         |
| How to use Avaya installation documents . . . . .                              | 8         |
| Pre-installation requirements . . . . .  | 9         |
| PNC license settings for S8700-series Servers . . . . .                        | 9         |
| Preinstallation tasks to complete at the customer site . . . . .               | 9         |
| Verifying that all the required equipment is on site . . . . .                 | 9         |
| Ensuring that the preinstallation tasks are complete . . . . .                 | 10        |
| Equipment specifications . . . . .   | 10        |
| About S8730 Server configurations . . . . .                                    | 13        |
| About RAID. . . . .  | 13        |
| About server port connections . . . . .  | 13        |
| S8700-series port connections . . . . .  | 14        |
| About modem connections . . . . .  | 19        |
| Modem options . . . . .  | 20        |
| About media gateways . . . . .   | 20        |
| About Processor Ethernet . . . . .   | 20        |
| About software duplication . . . . .   | 21        |
| About SSH . . . . .  | 21        |
| <b>Chapter 2: SNMP configuration</b> . . . . .                                 | <b>23</b> |
| Configuring the SNMP modules in the UPS . . . . .                              | 23        |
| Default UPS IP addresses for S8700-series Servers . . . . .                    | 24        |
| Prerequisites for configuring the SNMP module . . . . .                        | 25        |
| Administering the SNMP modules . . . . .                                       | 26        |
| Setting selected traps (alarming) . . . . .                                    | 26        |
| Configuring the SNMP subagent in the Avaya Ethernet switch (if used) . . . . . | 27        |
| Default IP addresses for the Ethernet switch . . . . .                         | 27        |
| Preparing to configure the Ethernet switch . . . . .                           | 28        |
| Configuring the Ethernet switch . . . . .                                      | 29        |
| <b>Chapter 3: Communication Manager installation</b> . . . . .                 | <b>31</b> |
| Clearing the ARP cache on the laptop . . . . .                                 | 31        |
| Applying power to the server . . . . .   | 32        |
| Accessing the server . . . . .   | 32        |
| Configuring Telnet for Windows 2000 and Windows XP . . . . .                   | 32        |
| Installing Avaya Communication Manager . . . . .                               | 33        |

|   |           |
|---|-----------|
| <b>Chapter 4: Server configuration</b>                            | <b>35</b> |
| Opening the Maintenance Web Interface.                            | 36        |
| Copying files to the server                                       | 36        |
| Creating a super-user login.                                      | 36        |
| Methods of Configuring a server                                   | 37        |
| Configuring the server manually                                   | 37        |
| Setting the date, time, and time zone.                            | 37        |
| Maintenance Web Pages configuration screens.                      | 38        |
| Ethernet interface assignments.                                   | 40        |
| Performing the manual configuration                               | 40        |
| Avaya Installation Wizard   | 41        |
| About the Avaya Installation Wizard                               | 41        |
| Running the Avaya Installation Wizard.                            | 42        |
| Verifying the server connection to the customer LAN (if provided) | 42        |
| Configuring the modem   | 43        |
| Configuring memory for an S8720 Server                            | 44        |
| Ensuring ESS and LSP compatibility.                               | 45        |
| Enabling firewall settings  | 46        |
| Enabling network time servers                                     | 46        |
| Configuring the NIC   | 47        |
| Release the server  | 48        |
| Configuring a second server                                       | 48        |
| Interchanging servers   | 48        |
| Accessing the standby server                                      | 48        |
| Interchanging servers   | 49        |
| Performing an integrity check on the active server                | 49        |
| <b>Chapter 5: IP interface translations</b>                       | <b>51</b> |
| Inputting initial system translations                             | 51        |
| Adding media gateways   | 52        |
| Enabling the IPSI.  | 53        |
| Adding the IPSI to the system                                     | 54        |
| Enabling IPSI duplication (duplicated control network only)       | 55        |
| Setting the alarm activation level                                | 55        |
| Saving translations   | 55        |
| <b>Chapter 6: IP interface configuration</b>                      | <b>57</b> |
| Connecting to the IPSIs   | 57        |

|   |           |
|---|-----------|
| IPSI address configuration . . . . .                                  | 57        |
| Programming the IPSI for static addressing . . . . .                  | 58        |
| Setting the VLAN and diffserv parameters . . . . .                    | 61        |
| Programming the IPSI for DHCP addressing . . . . .                    | 62        |
| Verifying connectivity to the server . . . . .                        | 65        |
| Verifying that the IPSIs are translated . . . . .                     | 65        |
| Upgrading the IPSI firmware version (if necessary) . . . . .          | 65        |
| Enabling control of the IPSIs . . . . .                               | 65        |
| Verifying the license status . . . . .                                | 66        |
| <b>Chapter 7: Postinstallation administration . . . . .</b>           | <b>67</b> |
| Verifying translations . . . . .                                      | 67        |
| Setting rules for daylight savings time . . . . .                     | 68        |
| Setting locations (if necessary) . . . . .                            | 69        |
| Verifying the date and the time (main server only) . . . . .          | 70        |
| Clearing and resolving alarms . . . . .                               | 71        |
| Enabling and disabling the Ethernet switch ports . . . . .            | 71        |
| Enabling alarms to INADS by way of a modem . . . . .                  | 72        |
| Enabling alarms to INADS by way of the SNMP module . . . . .          | 73        |
| Backing up files to the compact flash media . . . . .                 | 73        |
| Before leaving the site . . . . .                                     | 74        |
| <b>Chapter 8: Installation verification . . . . .</b>                 | <b>75</b> |
| Testing the IPSI circuit pack . . . . .                               | 75        |
| Testing the license file . . . . .                                    | 75        |
| S8730 LEDs . . . . .  | 76        |
| S8710 and S8720 LEDs . . . . .  | 77        |
| Additional server LED information . . . . .                           | 79        |
| Avaya C360 Ethernet switch LEDs . . . . .                             | 80        |
| UPS LEDs . . . . .  | 81        |
| TN2312BP IPSI LEDs . . . . .  | 82        |
| <b>Appendix A: Server access . . . . .</b>                            | <b>87</b> |
| Accessing the command line interface of the server with SSH . . . . . | 87        |
| Connecting to the server directly . . . . .                           | 89        |
| Connecting to the server remotely over the network . . . . .          | 92        |
| Connecting to the server remotely over a modem . . . . .              | 92        |

## Contents

|   |            |
|---|------------|
| Finding the IP address of the active server . . . . .   | 93         |
| Accessing the Maintenance Web Interface . . . . .   | 93         |
| Using the SAT command line prompt . . . . .   | 94         |
| Logins for Avaya technicians and BusinessPartners . . . . .   | 95         |
| Configuring the network for Windows 2000 and XP . . . . .   | 95         |
| Setting the browser options for Internet Explorer 6.0 . . . . .                                     | 96         |
| <b>Appendix B: Installation troubleshooting . . . . .</b>   | <b>97</b>  |
| Troubleshooting the installation of the server hardware . . . . .                                   | 97         |
| Troubleshooting the configuration of the server hardware . . . . .                                  | 98         |
| Troubleshooting the installation of the license file and<br>the Avaya authentication file . . . . . | 100        |
| <b>Index . . . . .</b>  | <b>101</b> |

# Chapter 1: Introduction

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

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

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

This installation document includes the following information:

- [Pre-installation requirements](#) on page 9
- [Configuring the SNMP modules in the UPS](#) on page 23
- [Server configuration](#) on page 35
- [IP interface translations](#) on page 51
- [IP interface configuration](#) on page 57
- [Postinstallation administration](#) on page 67
- [Installation verification](#) on page 75
- [Server access](#) on page 87
- [Installation troubleshooting](#) on page 97

---

## Audience

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

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

## How to use Avaya installation documents

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

To complete this installation:

- In this document, see:
  - [Pre-installation requirements](#) on page 9 first. This section describes the tasks that you must complete at the site before you start the installation.
  - [Equipment specifications](#) on page 10 for the technical specifications for the hardware.
- For how to install and connect the hardware, see *Quick Start for Hardware Installation: Avaya S8700-Series Server* (555-245-701).
- Return to this document and see the remaining sections in the following sequence to install the components of the server. If you are not to install certain components, skip the procedures for those components.
  - [Configuring the SNMP modules in the UPS](#) on page 23
  - [Server configuration](#) on page 35
  - [IP interface translations](#) on page 51
- See the appropriate sections in the following documents to install the port networks and the media gateways:
  - *Installing the Avaya G650 Media Gateway* (03-300144)
  - *Installation and Configuration for the Avaya G150 Media Gateway* (03-300395)
  - *Quick Start for Hardware Installation: Avaya G250 Media Gateway* (03-300433)
  - *Quick Start for Hardware Installation: Avaya G350 Media Gateway* (03-300148)
  - *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
  - *Installing and Upgrading the Avaya G250 Media Gateway* (03-300434)
  - *Installing and Upgrading the Avaya G350 Media Gateway* (03-300394)
  - *Installing and Upgrading the Avaya G450 Media Gateway* (03-602054)
  - *Quick Start for Hardware Installation: Avaya S8300 Server and Avaya G700 Media Gateway* (555-233-150)
  - *Installation and Upgrade for the Avaya G700 Media Gateway and Avaya S8300 Server* (555-234-100)
  - *Avaya IA 770 INTUITY AUDIX Messaging Application Administering the S8300 and S8400 Servers to work with IA 770*
- Return to this document and see:
  - [IP interface configuration](#) on page 57 to program the IP interface.



- [Postinstallation administration](#) on page 67
- [Installation verification](#) on page 75
- [Server access](#) on page 87
- [Installation troubleshooting](#) on page 97 if problems occur during the installation.

---

## Pre-installation requirements

This section describes the tasks that you must complete before you start the installation. You complete certain tasks before you go on site and other tasks at the site.

---

### PNC license settings for S8700-series Servers

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

---

### Preinstallation tasks to complete at the customer site

Before you start the installation, you must:

- Verify that all the required equipment is on site
- Ensure that the preinstallation team completed the preinstallation tasks
- Install the DAL2 card, if used

---

### Verifying that all the required equipment is on site

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

## Ensuring that the preinstallation tasks are complete

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

- Verify that the required number of open, customer-supplied, EIA-310D (or equivalent) standard 19-in. (48-cm) 4-post equipment rack(s) is(are) properly installed and solidly secured. Ensure that the screws that come with the racks are present. If you use a rack cabinet, ensure that the cabinet has adequate ventilation.
- Verify that the rail kit to support the server is available to install.
- Verify that the rail kit that is required to support the UPS is installed on the rack or available to install. For how to install the rails, see the documentation that comes with the rail kit.
- Verify that the equipment racks are grounded per local code. See *Job Aid: Approved Grounds* (555-245-772).
- Verify that the customer-provided AC power to the rack is from a nonswitched outlet.
- Verify that cables for the TN2312BP (IPSI) circuit packs are labeled and run from the control hardware rack to the port networks or that appropriate connectivity is provided.

## Equipment specifications

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

**Table 1: Control network components specifications**

| Component                           | Dimensions<br>English<br>(height x width x depth<br>in inches) | Dimensions<br>Metric<br>(height x width x depth<br>in centimeters) | Height<br>(u) | Weight<br>(lb/kg) |
|-------------------------------------|--|--|---------------|-------------------|
| Server<br>S8710, S8720, or<br>S8730 | 3.4 x 17.5 x 26  | 8.6 x 45 x 66  | 2             | 60/27<br>(loaded) |
| Ethernet switch:<br>C363T           | 1.75 x 17 x 14.4   | 4 x 43 x 37  | 1             | 11/5              |
| C364T                               | 1.75 x 17 x 14.4   | 4 x 43 x 37  | 1             | 11/5              |
| UPS:<br>700 VA                      | 3.5 x 17 x 19  | 9 x 43 x 48  | 2             | 34/15             |
| 1500 VA                             | 3.5 x 17 x 24  | 9 x 43 x 61  | 2             | 50/23             |

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

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

| Feature                         | Description   |
|---------------------------------|---|
| Microprocessor                  | S8710: 1 Intel Xeon<br>S8720: 1 AMD Opteron<br>S8730 1 Dual Core rev "F" AMD  |
| Memory                          | S8710: 512 MB<br>S8720: 1 GB<br>S8730: 4 GB   |
| Drives (SCSI)                   | Hard disk drive: 72 GB, 10,000 RPM<br>CD-ROM/DVD-ROM: 24x maximum<br>Diskette drive: 1.44 MB (3.5 in. [9 cm])   |
| DAL2 hardware duplication cards | Used for the hardware duplication configuration only. Not used for the software duplication configuration.  |
| Physical dimensions             | S8710/S8720:<br>Height: 3.4 inches [8.6 cm], 2 U)<br>Depth: 26 inches (66 cm)<br>Width: 17.5 inches (45 cm)<br>Maximum weight: 60 lb (27 kg)<br><br>S8730:<br>Height: 3.38 inches [8.59 cm], 2 U)<br>Depth: 26.01 inches (66.07 cm)<br>Width: 17.54 inches (44.54 cm)<br>Maximum weight: 60 lb (27.22 kg) |
| Integrated functions            | S8710/8720: 2 10/100/1000BaseT Ethernet connectors<br>S8730: 2 100/1000Gb Ethernet ports<br>Serial connector<br>iLO connector (unused)<br>Keyboard connector<br>Mouse connector<br>USB connectors:<br>S8710: 2<br>S8720: 3<br>S8730: 4<br><br>Video connector<br>VHDCI SCSI connector                     |

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

**Table 3: S8710/S8720/S8730 Server environmental specifications**

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

---

## About S8730 Server configurations

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

For different configurations of the S8730 Server:

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

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

---

## About RAID

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

**Note:**

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

---

## About server port connections

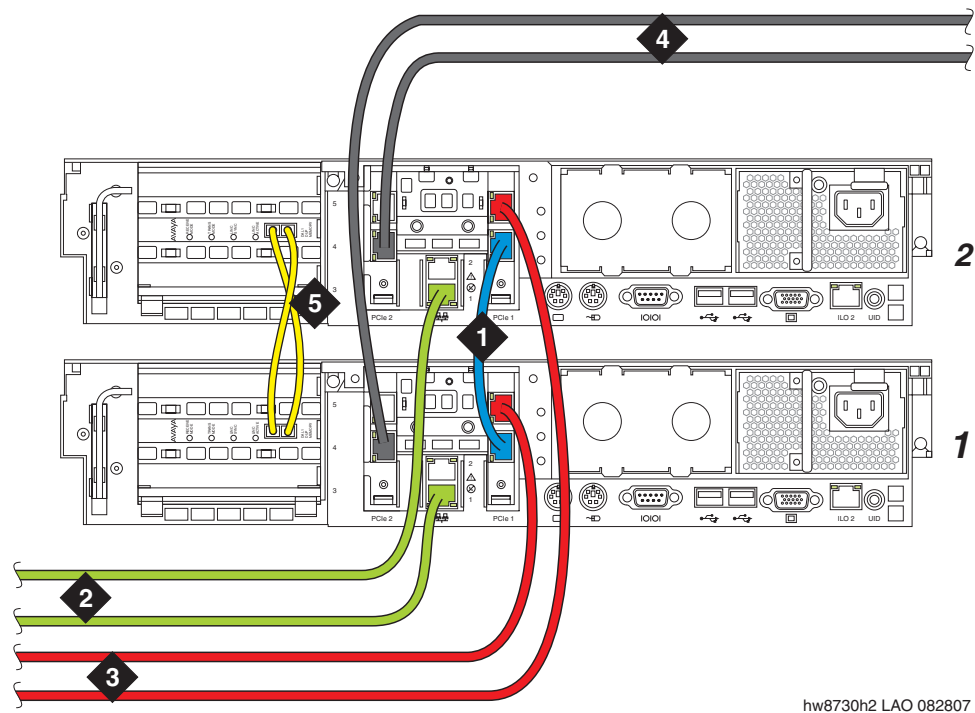
The following section explains how to connect the Ethernet ports on the back of the server.

## S8700-series port connections

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

- For a guide to connect the cables to the servers for hardware duplication on the S8730 Server, see [Figure 1: Duplication and control network cabling for hardware duplication \(S8730\)](#) on page 15.
- For a guide to connect the cables to the servers for hardware duplication on the S8720 or S8710 Server, see [Figure 2: Duplication and control network cabling for hardware duplication \(S8720/S8710\)](#) on page 16.
- For a guide to connect the cables to the servers for software duplication on the S8730 Server, see [Figure 3: Duplication and control network cabling for software duplication \(S8730\)](#) on page 17.
- For a guide to connect the cables to the servers for software duplication on the S8720 or S8710 Server, see [Figure 4: Duplication and control network cabling for software duplication \(S8720/S8710\)](#) on page 18.

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



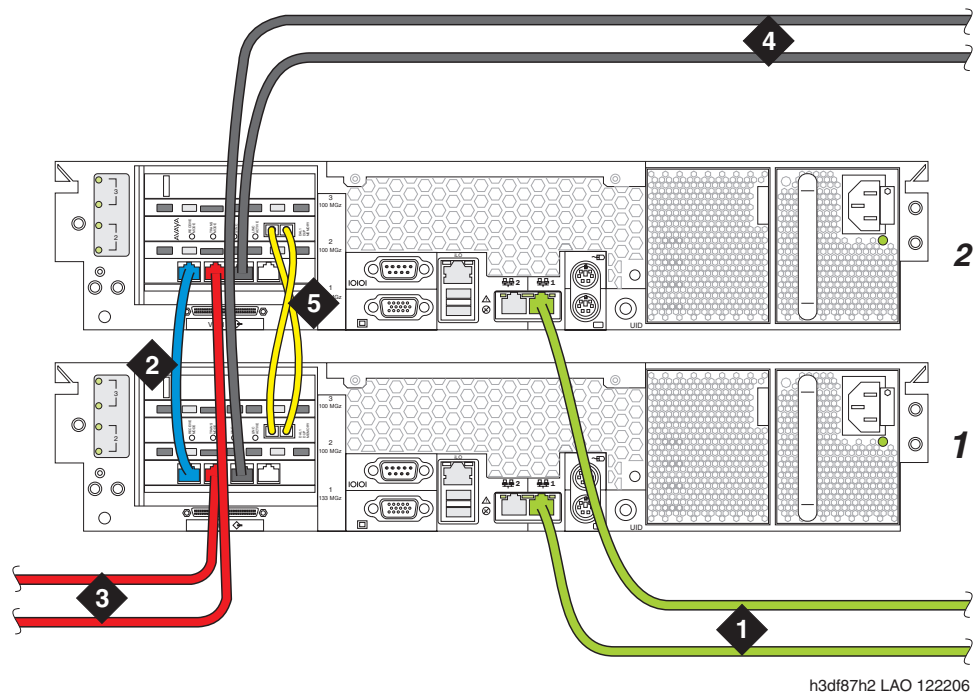
**Figure notes:**

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

**Note:**

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

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



h3df87h2 LAO 122206

**Figure notes:**

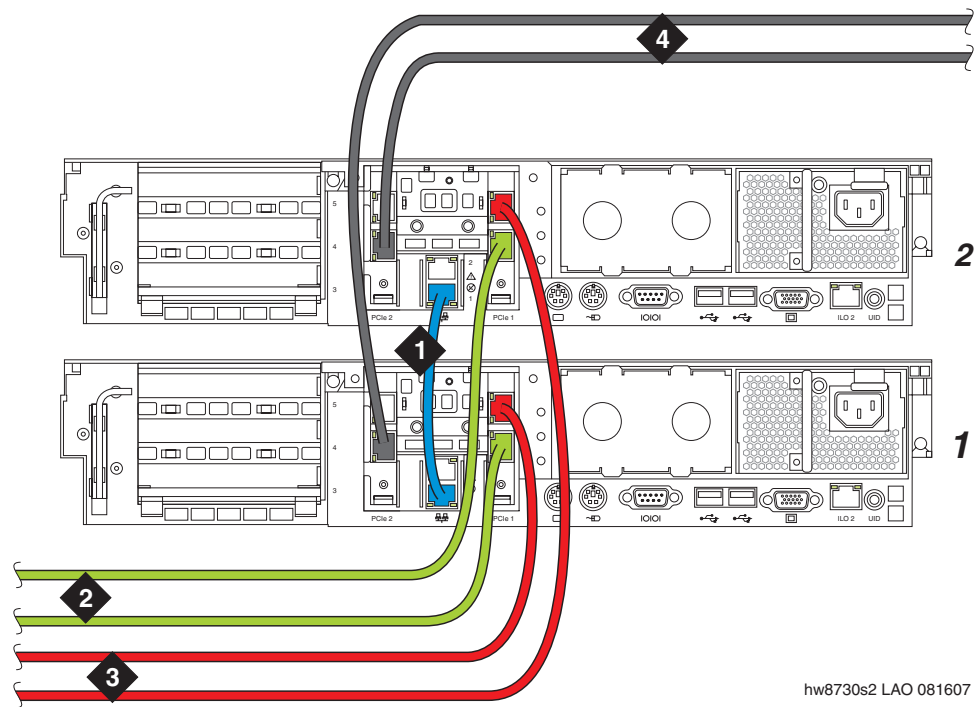
1. Eth0 — To an Ethernet switch and/or the corporate LAN for control network A (CNA)
2. Eth2 — Server Duplication Link
3. Eth3 — To an Ethernet switch and/or the corporate LAN for control network B (CNB)
4. Eth4 — To the customer LAN if the control networks are dedicated
5. Fiber duplication cable

**Note:**

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



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



hw8730s2 LAO 081607

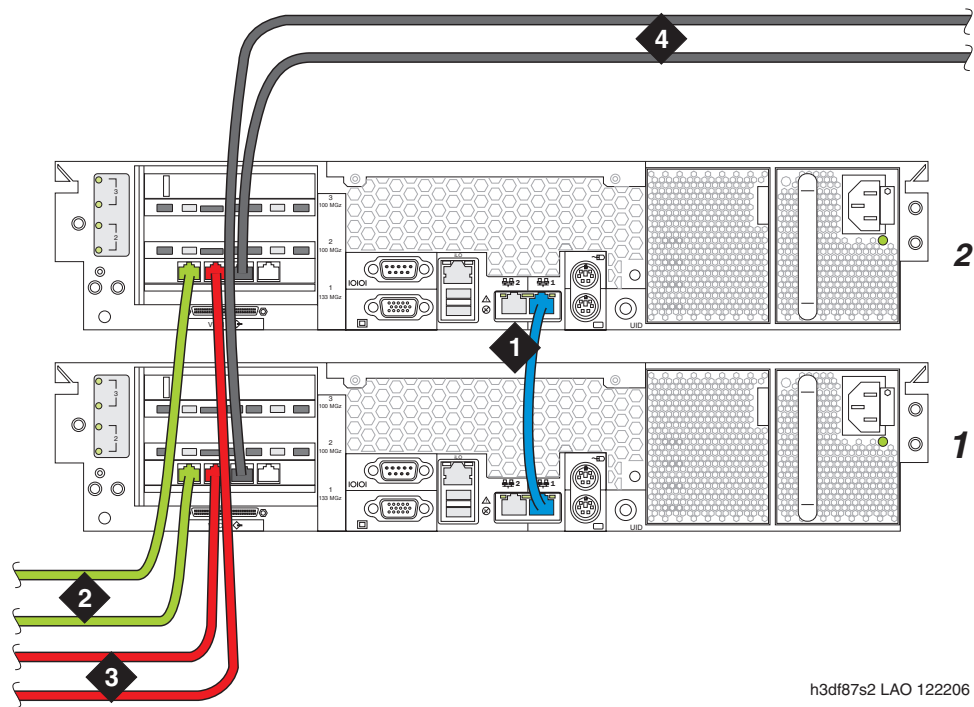
**Figure notes:**

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

**Note:**

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

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



h3df87s2 LAO 122206

**Figure notes:**

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

**Note:**

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

---

## About modem connections

**Note:**

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

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

**CAUTION:**

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

---

## Connecting to collocated servers

**Important:**

Both servers share one telephone line.

To connect modems to collocated servers:

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

---

## Connecting to separated servers

**Important:**

Each server has a dedicated telephone line.

To connect to separated servers:

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

## Modem options

You set the modem options when you configure the server. You do not set options on the modems themselves.

---

## About media gateways

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

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

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

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

---

## About Processor Ethernet

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

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

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

---

## About software duplication

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

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

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

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

---

## About SSH

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

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

You can use SSH to access the following devices:

- The S8300, S8400, S8500, and S8700-series Servers on Release 3.1 or later of Communication Manager

**Note:**

With Release 4.0 or later of Communication Manager, Telnet is disabled, so you must use SSH to access the servers after Communication Manager software Release 4.0 or later is installed.

- A Maintenance Processor Complex (MPC), which is used with the S8400 Server
- A TN2312BP IPSI that is running firmware version 20 or higher
- A TN8412AP SIPI

## Chapter 1: Introduction

- A TN2602 IP Media Resource that is running firmware version 212 or higher
- An Expanded Meet-Me Conferencing (EMMC) server
- A SIP Enablement Services (SES) server
- G250, G350, and G450 media gateways
- C360 Ethernet switches



### **Important:**

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

## Chapter 2: SNMP configuration

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

**Important:**

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

---

### Configuring the SNMP modules in the UPS

**Important:**

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

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

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

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

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

## Default UPS IP addresses for S8700-series Servers

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



### Important:

Do not use the IP address of the active server.

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

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



### Important:

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

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



---

## Prerequisites for configuring the SNMP module

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

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

**Note:**

Avaya Terminal Emulation and HyperTerminal are supported terminal emulation applications.

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



**SECURITY ALERT:**

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

For information about which traps to set, see [Setting selected traps \(alarming\)](#) on page 26.

- If the control network is nondedicated, ensure that the 162/udp port for input to server is enabled and the default is disabled. If you do not enable the 162/udp port and disable the default, the server cannot receive the traps from either UPS. See [Enabling firewall settings](#) on page 46.

---

## Administering the SNMP modules

**Note:**

Use the default IP addresses.

1. Connect the RS-232 serial port of your Services laptop computer to the DB-9 connector on the back of the SNMP module for UPS1 using the DB-9 to DB-9 serial cable that is supplied with the SNMP module.
2. Open a VT-100 terminal emulation session on your computer.
3. Set the IP address for the UPS.
4. Set the subnet mask for the UPS.
5. Set the gateway address for the UPS.
6. Set the IP address of the trap receiver for the UPS.
7. Set the SNMP community name string for Get, Set, and Trap. For information on which traps to set, see [Setting selected traps \(alarming\)](#) on page 26.
8. When finished, disconnect your computer from the UPS.
9. Connect one end of a CAT5 straight-through cable to the RJ45 connector on the UPS1 SNMP module and the other end of the cable to the next available port on the Ethernet switch for Control Network A (CNA).

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

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

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

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

---

## Setting selected traps (alarming)

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

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

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

---

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

### Important:

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

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

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

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

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

### Note:

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

---

## Default IP addresses for the Ethernet switch

For how to administer the SNMP subagent in the Ethernet switches see [Configuring the Ethernet switch](#) on page 29. If the control network is duplicated, perform the same steps for both Ethernet switches.

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

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



**Important:**

Do not use the IP address of the active server.

**Table 5: Default values for a dedicated control network**

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

---

## Preparing to configure the Ethernet switch

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

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

**Note:**

Avaya Terminal Emulation and HyperTerminal are supported terminal emulation applications.

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

 **SECURITY ALERT:**

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

- If the control network is not dedicated, ensure that the 162/udp port for input to server is enabled and the default is disabled. If you do not enable the 162/udp port and disable the default, the server cannot receive the traps from either UPS. See [Enabling firewall settings](#) on page 46.

---

## Configuring the Ethernet switch

**Note:**

Use the default addresses.

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

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

**Note:**

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

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

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

# Chapter 3: Communication Manager installation

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

This chapter covers the following tasks:

- [Clearing the ARP cache on the laptop](#) on page 31
- [Applying power to the server](#) on page 32
- [Accessing the server](#) on page 32
- [Configuring Telnet for Windows 2000 and Windows XP](#) on page 32
- [Installing Avaya Communication Manager](#) on page 33

---

## Clearing the ARP cache on the laptop

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

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

If the ARP cache does not contain the specified IP address, the 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.

## Applying power to the server

**Note:**

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

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

---

## Accessing the server

1. Use a cross-over cable to connect your laptop computer to the Services port on the back of the server. The Services port is labeled "2" and is configured as Eth1.
2. Wait at least 3 minutes after you turn on the server before you start a Telnet session to access the information on the CD-ROM.

---

## Configuring Telnet for Windows 2000 and Windows XP

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

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

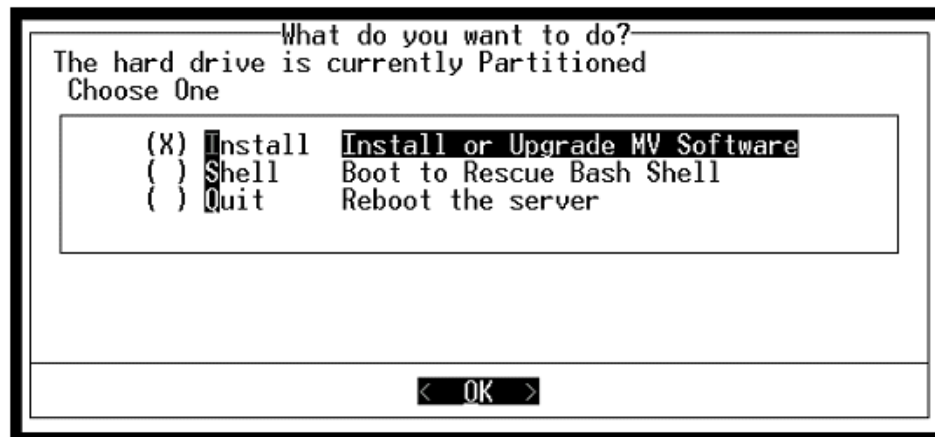


---

## Installing Avaya Communication Manager

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

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



**Note:**

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

3. Select **Install**, ensure that **<OK>** is highlighted, and press **Enter**.
4. On the Select Release Version screen, ensure that the Build line and **<OK>** are highlighted.
5. Press **Enter** to partition the hard disk drive and format the partitions.  
Once the drive is properly configured, the program starts the installation process and reports the progress.  
These processes can take up to 20 minutes to complete.
6. You must remove the CD-ROM from the drive at this time. When the server is ready to reboot, the drawer of the CD-ROM drive opens.  
The reboot can take up to 3 minutes. The Telnet session drops automatically when the reboot starts.



# Chapter 4: Server configuration

After you install the Communication Manager software, you must use the Avaya Installation Wizard to configure the server.

This section covers the following tasks:

- [Copying files to the server](#) on page 36
- [Creating a super-user login](#) on page 36
- [Configuring the server manually](#) on page 37
- [Running the Avaya Installation Wizard](#) on page 42
- [Verifying the server connection to the customer LAN \(if provided\)](#) on page 42
- [Configuring the modem](#) on page 43
- [Configuring memory for an S8720 Server](#) on page 44
- [Enabling firewall settings](#) on page 46
- [Enabling network time servers](#) on page 46
- [Release the server](#) on page 48
- [Configuring a second server](#) on page 48

**Note:**

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

**Note:**

Ensure that your networking and Web browser settings are correct. For more information, see [Configuring the network for Windows 2000 and XP](#) on page 95.

## Opening the Maintenance Web Interface

You can use the Maintenance Web Interface to copy license files and authentication files, service packs, and update files from the Services laptop to the server. For how to open the Maintenance Web Interface, see [Finding the IP address of the active server](#) on page 93.

---

## Copying files to the server

1. From the Maintenance Web Interface, under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the Choose File window on your computer. Find the files that you need to copy to the server.
4. Click **Download** to copy the files to the server.

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

---

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

**Note:**

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

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

---

## Methods of Configuring a server

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

1. [Configuring the server manually](#) on page 37 using Integrated Management Maintenance Web Pages
2. The Avaya Installation Wizard with the Electronic Pre-installation Worksheet (EPW)
3. The Avaya Installation Wizard interactively

---

## Configuring the server manually

### Setting the date, time, and time zone



**Important:**

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

## Chapter 4: Server configuration

To set the date, time, and time zone:

1. From the Main Menu, under Server, click **Server Date/Time**.
2. In the **Server Date/Time** window, verify the date and time are correct. If the date and time are incorrect:
  - a. Enter the date
  - b. Enter the time
  - c. Enter the time zone
  - d. Click **Submit**



### **WARNING:**

If you set time zone, you must reboot the server.

- e. Reboot the server:
  1. Click Shutdown Server under the Server heading.
  2. Select Delayed Shutdown and Restart server after shutdown.
  3. Click Shutdown.

You will be logged off the server when it reboots. You can use ping to verify when the server is accessible again.

## Maintenance Web Pages configuration screens

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

**Table 6: S8700-Series Server configuration web pages**

| Page                          | S8700-series Main | S8700-series ESS |
|-------------------------------|-------------------|------------------|
| Set Identities                | ✓                 | ✓                |
| Configure Interfaces          | ✓                 | ✓                |
| Configure ESS                 | ✓                 | ✓                |
| Configure Memory (S8720 only) | ✓                 | ✓                |
| Configure Switches            | ✓                 | ✓                |

**Table 6: S8700-Series Server configuration web pages**

| Page                  | S8700-series Main | S8700-series ESS |
|-----------------------|-------------------|------------------|
| Set DNS/DHCP          | ✓                 | ✓                |
| Set Static Routes     | ✓                 | ✓                |
| Configure Time Server | ✓                 | ✓                |
| Set Modem Interface   | ✓                 | ✓                |

The following describes each of the configuration pages:

- **Set Identities** — Use this page to assign Avaya server host names and to assign server functions to a physical Ethernet interface. The options are pre populated with defaults, but should be changed as needed for the customer's configuration. See [Ethernet interface assignments](#) on page 40 for a guide to assigning functions to Ethernet interfaces.
- **Configure Interfaces** — Use this page to enter the IP address, subnet mask, gateway, and speed for the management LAN and control network.
- **Configure ESS/LSP** — Use this page to configure the server as either a primary controller for the system or as an Enterprise Survivable Server (ESS) or a Local Survivable Processor (LSP).
- **Configure Memory** — For the S8720 main or ESS server, S8710 ESS server, use this page to configure the server as either standard or extra large. A server that is configured as extra large provides higher capacities.
- **Configure Switches** — Use this page to specify an IP address and optional SNMP community strings for any Ethernet adjuncts that the Avaya server controls, that are connected to the server over a private LAN.
- **Set DNS/DHCP** — Use this page to enable the different devices (endpoints) in your Avaya call-processing system to communicate over the corporate LAN. Most corporate networks have one or more domain name service (DNS) servers that associate an IP address with the name of a device. When you administer the DNS with the Avaya server names, you can access the servers by name and by IP address over the corporate network.
- **Set Static Routes** — Use this page only if the network administrator instructs you. If the administrator does not specify a particular route for the server to send information over the network, leave the options blank and click **Continue**.
- **Configure Time Server** — Use this page to specify the time source that the Avaya server uses to set the time of day.
- **Set Modem Interface** — Use this page to enable Avaya services or another trouble-tracking service to monitor the Avaya server for alarms. Technical-support representatives can dial in to this interface to fix problems as they occur.

## Ethernet interface assignments

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

**Table 7: S8700-series Server Ethernet assignments**

|                          | S8710/S8720/<br>S8730 hardware<br>duplication and<br>dedicated control<br>network | S8720/S8730<br>software<br>duplication with<br>dedicated control<br>network | S8710/S8720/<br>S8730 hardware<br>duplication with<br>non-dedicated<br>control network | S8720/S8730<br>software<br>duplication with<br>non-dedicated<br>control network |
|--------------------------|---|---|--|---|
| <b>Control network A</b> | eth0  | eth2  | eth0   | eth2  |
| <b>Control network B</b> | eth3 (if used)  | eth3 (if used)  | eth3 (if used)   | eth3 (if used)  |
| <b>LAN</b>               | eth4  | eth4  | eth0   | eth2  |
| <b>Duplication Link</b>  | eth2  | eth0  | eth2   | eth0  |

## Performing the manual configuration

To configure the server using the manual method:

1. Log into the server and bring up the Integrated Management Maintenance Web Pages.
2. From the Main Menu, under Server Configuration and Upgrades click **Configure Server**.
3. Click through the Review Notices to get to the Select Method for Configuring Server page.
4. Select "Configure all services using the wizard" and click continue to get to the Set Server Identities page.
5. Fill in the fields on the Set Identities page and subsequent pages:
  - Configure Interfaces
  - Configure ESS
  - Configure Memory (S8720 only)
  - Configure Switches
  - Set DNS/DHCP
  - Set Static Routes
  - Configure Time Server
  - Set Modem Interface



- Update System

Use your pre-installation planning forms to enter information on these pages. For more information on these pages, see [Configuring the server manually](#) on page 37 or click on the Help button at the bottom of each page.

6. When you complete all the fields, click Continue on the Update System page. The Update System page displays each configuration task as it completes it. The last line says, "System modifications completed."

---

## Avaya Installation Wizard

### About the Avaya Installation Wizard

Use the Avaya Installation Wizard to:

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

**Note:**

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

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

The Avaya Installation Wizard cannot be used to configure:

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

**Note:**

To configure XL or Standard Memory, use the Configure Server in the Integrated Management Maintenance Web Pages. For more information see, [Configuring memory for an S8720 Server](#) on page 44.

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

**Note:**

To configure Software Duplication, use the Configure Server in the Integrated Management Maintenance Web Pages.

To use the Installation Wizard, you can either:

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

### Running the Avaya Installation Wizard

1. With the Web browser open, type **192.11.13.6** and press **Enter** in the browser address window to display the login page.
2. Log in as **craft** and use the initial craft password.
3. Click **Launch Avaya Installation Wizard**.
4. Follow the prompts. For more information use **Help** on each page.



#### **CAUTION:**

The license settings for the platform and the port network connectivity (PNC) attributes for the S8700-series Server can be complex. For more information, see [PNC license settings for S8700-series Servers](#) on page 9.



#### **WARNING:**

If the time zone is set in the AIW, you must reboot the server after AIW completes.

5. 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.

---

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

1. From the Maintenance Web Interface, under Diagnostics, click **Ping**.
2. Select **Host Name Or IP Address** and type the IP address of a computer on the network.
3. Click **Execute Ping**.

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

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

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

---

## Configuring the modem

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

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

7. Click **Change**.

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

---

## Configuring memory for an S8720 Server

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

**Note:**

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

**Note:**

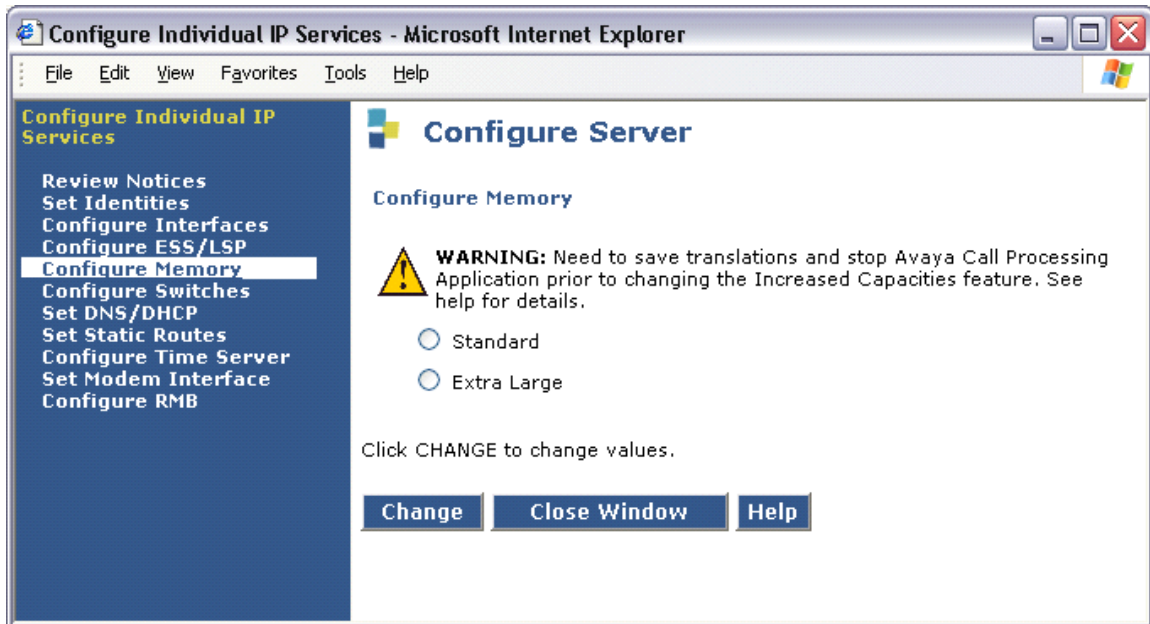
If the main servers are S8720 configured as Extra Large (XL), ESSs and LSPs must be configured as XL. See [Ensuring ESS and LSP compatibility](#) on page 45.

1. Before configuring the memory, stop Communication Manager by running the bash command `stop -acf`.
2. From the Maintenance Web Interface, under Server Configuration, click **Configure Server**.
3. Click **Continue** until you get to the **Specify how you want to use this wizard** page.



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

- **Configure ESS** (if an ESS server)



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

---

## Ensuring ESS and LSP compatibility

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

## Enabling firewall settings

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

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

---

## Enabling network time servers

### **Important:**

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

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

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

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

**Note:**

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

When the Avaya Installation Wizard prompts you for information about the network time servers, enter the DNS name or the IP address for the primary network time server and the secondary and the tertiary time servers if any. If you enter a DNS name instead of an IP address for the network time server, you must specify the IP address of the DNS server on the DNS/DHCP web page. For more information, see [About the Avaya Installation Wizard](#) on page 41.

For more information about NTP, see RFC 958.

---

## Configuring the NIC

1. From the Maintenance Web Interface, under Server Configuration, click **Configure Server**.
2. Click **Continue** until you get to the "Specify how you want to use this Wizard" page.

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

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

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

**Successfully configured ethernet interfaces.**

---

## Release the server

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

---

## Configuring a second server

Use the same procedures that you used to configure the first server. Repeat [Clearing the ARP cache on the laptop](#) on page 31 through [Release the server](#) on page 48 for the second server.

---

## Interchanging servers

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

---

## Accessing the standby server

To access the standby server:

1. Clear the ARP cache on the laptop if necessary. For more information, see [Clearing the ARP cache on the laptop](#) on page 31 and return here.
2. Connect the laptop to the Services port (2) on the back of the server with a cross-connect CAT5 cable.
3. Open a browser and connect to the active server.
4. If you are not already logged in to the Maintenance Web Interface, log in. For more information, see [Accessing the Maintenance Web Interface](#) on page 93.



---

## Interchanging servers

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

1. Under Server, click **Interchange Servers**.
2. Verify the settings in the following fields:
  - **Standby Busied:** no
  - **Standby Refreshed:** yes
  - **Standby Shadowing:** on
  - **Duplication Link:** up
  - **Control Network health:** X/X/X for both servers, where X is the number of administered IPSI port networks. For more information, see [Chapter 5: IP interface translations](#) on page 51.
3. Click **Interchange**.

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

This server is now the active server.

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

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

---

## Performing an integrity check on the active server

To perform an integrity check on the active server:

1. On the Maintenance Web Interface, under Diagnostics, click **Server > Status Summary**.
2. Verify the following:
  - Mode: Active**
  - Server Hardware: okay**
  - Processes: okay**
3. Select **Server > Process Status**.
4. Under Frequency, click **Display Once**.
5. Click **View**.
6. Verify all operations are **UP**.



# Chapter 5: IP interface translations

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

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

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

Perform these tasks to administer IPSI circuit packs:

- [Inputting initial system translations](#) on page 51
- [Adding media gateways](#) on page 52
- [Enabling the IPSI](#) on page 53
- [Adding the IPSI to the system](#) on page 54
- [Enabling IPSI duplication \(duplicated control network only\)](#) on page 55
- [Setting the alarm activation level](#) on page 55
- [Saving translations](#) on page 55

---

## Inputting initial system translations

1. Open a SAT session. See [Using the SAT command line prompt](#) on page 94.
2. Enter translations:  
If the system translations were prepared offsite, enter the translations and reset the server.  
If the translations are not available, enter minimal translations to verify connectivity to the port networks.
3. After you enter the translations, type `save translation` and press **Enter** to save the translations to the hard disk drive.
4. Type `reset system 4` and press **Enter** to have the software read the copied translations.

## Adding media gateways

**Note:**

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

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

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

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

```

add cabinet 1
                                                    Page 1 of 1
                                                    CABINET
CABINET DESCRIPTION
    Cabinet: 1
    Cabinet Layout: G650-rack-mount-stack
    Cabinet Type: expansion-portnetwork
    Number of Portnetworks: 1
    Survivable Remote EPN? n
    Location: 1                IP Network Region:1
    Cabinet Holdover: A-carrier-only
    Room:                    Floor:                Building:

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

## Enabling the IPSI

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

```

change system-parameters ipserver-interface                               Page 1 of 1

                                IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS

SERVER INFORMATION

                                IPSI Host Name Prefix: birch
                                Primary Control Subnet Address: 198.152.254. 0 *
                                Secondary Control Subnet Address: 198.152.255. 0 *

OPTIONS

                                Switch Identifier: A
                                IPSI Control of Port Networks: enabled

```

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

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

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

## Adding the IPSI to the system

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

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

```

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

                                IP Control? y                Socket Encryption? n
Ignore Connectivity in Server Arbitration? n                Enable QoS? n
                                Administer secondary ip server interface board? y

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

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

```

```

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

                                IP Control? y                Socket Encryption? n
Ignore Connectivity in Server Arbitration? n                Enable QoS? n

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

```

3. Set the **IP Control** field to **y**.

4. Verify that all the other fields are populated and submit the form to save the changes.
5. Repeat this procedure for each port network.

---

## Enabling IPSI duplication (duplicated control network only)

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

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

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

---

## Setting the alarm activation level

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

---

## Saving translations

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





# Chapter 6: IP interface configuration

This chapter covers the following tasks:

- [Connecting to the IPSIs](#) on page 57
- [IPSI address configuration](#) on page 57
- [Programming the IPSI for static addressing](#) on page 58
- [Setting the VLAN and diffserv parameters](#) on page 61
- [Programming the IPSI for DHCP addressing](#) on page 62
- [Verifying connectivity to the server](#) on page 65
- [Verifying that the IPSIs are translated](#) on page 65
- [Upgrading the IPSI firmware version \(if necessary\)](#) on page 65
- [Enabling control of the IPSIs](#) on page 65
- [Verifying the license status](#) on page 66

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

---

## Connecting to the IPSIs

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

---

## IPSI address configuration

The IPSI circuit pack receives an IP address:

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

**Note:**

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

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

- [Programming the IPSI for static addressing](#) on page 58
- [Programming the IPSI for DHCP addressing](#) on page 62

---

## Programming the IPSI for static addressing

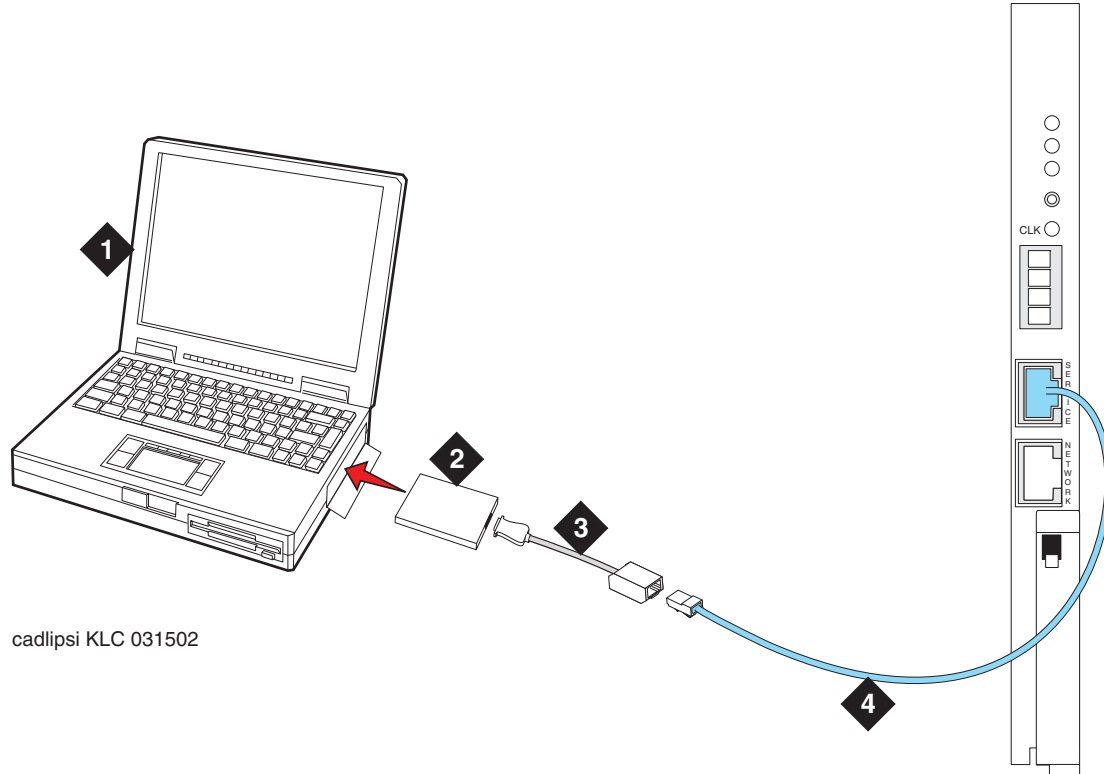


**Important:**

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

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

---

**Figure 5: Connecting the laptop directly to the IPSI**
**Figure notes:**

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

**Note:**

Ensure that you have the password before proceeding.

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

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

For information on how to use SSH, see [Accessing the command line interface of the server with SSH](#) on page 87.

**Note:**

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

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

**Note:**

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

6. Log in as `craft`.

Prompt = [IPADMIN]:

7. Type `show control interface` and press **Enter** and then type `show port 1` and press **Enter** to see the current control interface settings.
8. To set the control interface, type `set control interface ipaddr netmask` and press **Enter**, where `ipaddr` is the customer-provided IP address and `netmask` is the customer provided subnet mask.

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

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

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

[IPADMIN]: show control interface

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

[IPADMIN]: █
```

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

14. Log back in to the IPSI using SSH.
15. Use `show control interface` to verify the administration.
16. Type `exit` and press **Enter**.

---

## Setting the VLAN and diffserv parameters

1. Connect to the IPSI and log in as `craft`.
2. To display the quality of service values, type `show qos` and press **Enter**.
3. Use the `set` commands in the list below to set the VLAN, diffserv, and port parameters. If the customer does not specify different values, use these recommended values.

**Note:**

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

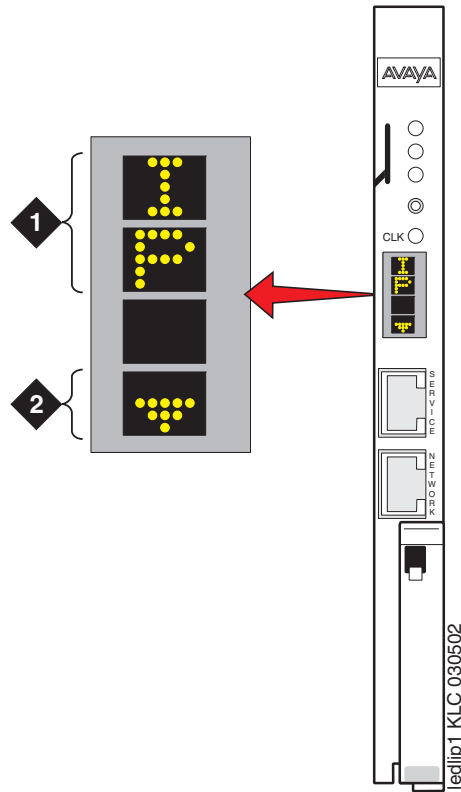


**Important:**

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

- `set vlan priority 6`
  - `set diffserv 46`
  - `set vlan tag on`
  - `set port negotiation 1 disable`
  - `set port duplex 1 full`
  - `set port speed 1 100`
4. Type `show qos` and press **Enter** to check the administered values.
  5. Type `reset` and press **Enter** to capture the updated parameter values.  
The reset terminates the administration session and automatically logs you out.
  6. Log in again and use the `show qos` command to ensure that the parameter settings are correct.
  7. Disconnect the laptop from the IPSIfaceplate.
  8. Check the LED on the IPSIfaceplate. Verify that the display shows the letters I and P and a filled-in V at the bottom. (See [Figure 6](#)).

Figure 6: IPSI LED display for static address



**Figure notes:**

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

**Note:**

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

9. Repeat this procedure for each IPSI circuit pack.

---

## Programming the IPSI for DHCP addressing



**Important:**

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

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

**Note:**

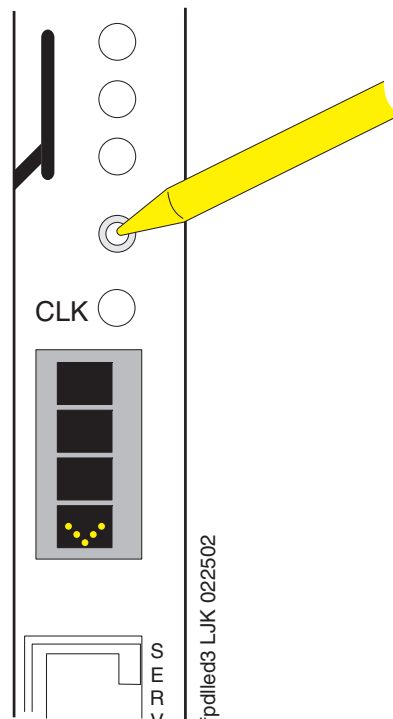
In the following procedure, you must start step 2 within 5 seconds after inserting the circuit pack.

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

**Note:**

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

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



**Note:**

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

**Note:**

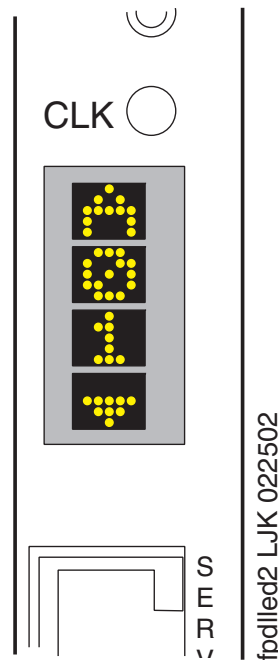
If you have only one system, the default switch ID is A. The second system is B and so on. The switch ID is *not* the media gateway or carrier letter.

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

**Note:**

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

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



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



---

## Verifying connectivity to the server

1. Open the Maintenance Web Interface and log in as **craft**.
2. Under Diagnostics, click **Ping** and select **Other server(s)**, **All IPSIs**, **UPS(s)**, **Ethernet switches** to verify connectivity to these units.
3. Click **Execute Ping**.
4. Verify that all endpoints respond correctly.

---

## Verifying that the IPSIs are translated

**Note:**

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

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

---

## Upgrading the IPSI firmware version (if necessary)

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

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

---

## Enabling control of the IPSIs

1. Ensure that the IPSIs have the same, current firmware.

2. For duplicated IPSIs, enable IPSI duplication before you enable IPSI control. See [Enabling IPSI duplication \(duplicated control network only\)](#) on page 55. On the SAT, type `change system-parameters ipserver-interface` and press **Enter**.
3. Ensure the **IPSI Control of Port Networks:** field is set to **enabled**.
4. Submit the screen to save the changes.

---

## Verifying the license status

On the Maintenance Web Interface, under Security, click **License File** and verify that the license mode is now normal.

# Chapter 7: Postinstallation administration

This section covers the following tasks:

- [Verifying translations](#) on page 67
- [Setting rules for daylight savings time](#) on page 68
- [Setting locations \(if necessary\)](#) on page 69
- [Verifying the date and the time \(main server only\)](#) on page 70
- [Clearing and resolving alarms](#) on page 71
- [Enabling and disabling the Ethernet switch ports](#) on page 71
- [Backing up files to the compact flash media](#) on page 73
- [Enabling alarms to INADS by way of a modem](#) on page 72
- [Enabling alarms to INADS by way of the SNMP module](#) on page 73
- [Before leaving the site](#) on page 74

---

## Verifying translations

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

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

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

## Setting rules for daylight savings time

You set the date, the time, and the time zone through the Maintenance Web Interface on the server. You must use SAT commands to set the rules for daylight savings time.

**Note:**

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

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

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

**Note:**

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

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

## Setting locations (if necessary)

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

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

```
change locations                                     Page 1 of 5
                                                    LOCATIONS
                                                    ARS Prefix 1 Required For 10-Digit NANP Calls? y
```

| Number | Name        | Timezone<br>Offset | Daylight-Savings<br>Rule | Number Plan<br>Area Code |
|--------|-------------|--------------------|--------------------------|--------------------------|
| 1      | <b>Main</b> | + 00:00            | 0                        |                          |
| 2      | CA          | - 02:00            | 0                        |                          |
| 3      |             | :                  |                          |                          |
| 4      |             | :                  |                          |                          |
| 5      |             | :                  |                          |                          |
| 6      |             | :                  |                          |                          |
| 7      |             | :                  |                          |                          |
| 8      |             | :                  |                          |                          |
| 9      |             | :                  |                          |                          |
| 10     |             | :                  |                          |                          |
| 11     |             | :                  |                          |                          |

2. In the ARS Prefix 1 Required for 10-Digit NANP Calls? field, type **y**.
3. Type the information in the various fields for each media gateway.  
In the Name field for location 1, type **Main**.
4. Click Submit to save the changes.

**Note:**

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

## Verifying the date and the time (main server only)

Use SAT commands to verify the date and time.

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

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

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

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

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

2. Verify that the date and the time of day are correct.
  - If the date and the time of day are correct, go to 5.
  - If the date and time of day are not correct, proceed to step 3.
3. Verify connectivity to any administered Network Time Server:
  - a. Using the Maintenance Web Interface, click **Network Time Sync** under **Diagnostics**. The Network Time Sync screen confirm synchronization to any administered Network Time Server.
  - b. Resolve any connection or administration issues related to the Network Time Server. If the Network Time Server is not administered:
    1. In the Maintenance Web Interface, click **Server Date/Time** under the Server heading. Set the correct date and the correct time. Verify that the time zone is correct.



### Important:

If you change the time zone, you must reboot the server.

4. Repeat this procedure, beginning with step 1.
5. Verify that the Daylight Savings Rule field is correct.
  - 0 if this server is in a location that does not use daylight savings time
  - 1-15 use an administered rule. The rule is administered using the SAT command `daylight-savings-rules`. For more information on the daylight-savings-rules, see [Setting rules for daylight savings time](#) on page 68.

**Note:**

The daylight savings rule setting on this form is the rule that is utilized by the Communication Manager software. Additional daylight savings rules can be implemented for the specific locations of hardware supported by the Communication Manager software. For more information, see [Setting locations \(if necessary\)](#) on page 69.

---

## Clearing and resolving alarms

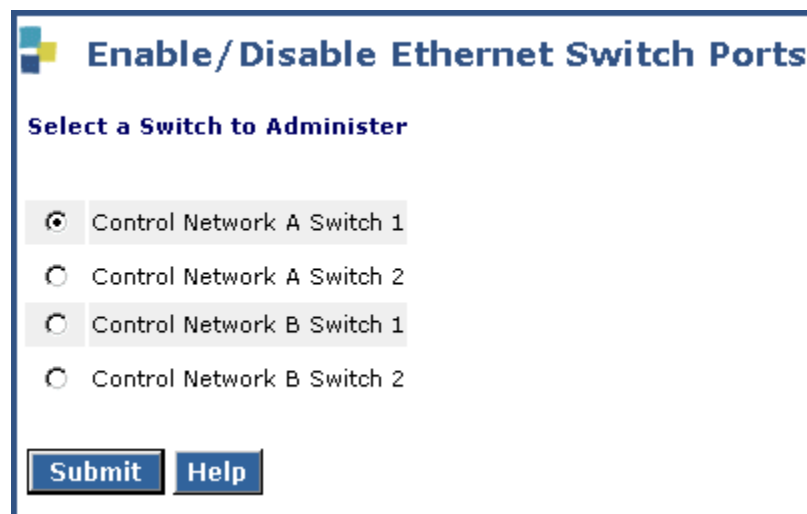
1. On the Maintenance Web Interface, under Alarms, click **Current Alarms**.  
You can resolve alarms on the *active* server only.
2. Select the server alarms to clear and click **Clear**.
3. Using SAT commands or other standard troubleshooting procedures, to resolve any major alarms.

---

## Enabling and disabling the Ethernet switch ports

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

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



**Enable/Disable Ethernet Switch Ports**

Select a Switch to Administer

Control Network A Switch 1

Control Network A Switch 2

Control Network B Switch 1

Control Network B Switch 2

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

**Enable/Disable Ports for Control Network A Switch 1**

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

**Submit Changes** **Help**

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

---

## Enabling alarms to INADS by way of a modem

**Note:**

Enable alarms on both servers.

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



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

---

## Enabling alarms to INADS by way of the SNMP module

**Note:**

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

To enable alarms on the servers:

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

---

## Backing up files to the compact flash media

**Note:**

Avaya requires the use of industrial grade compact flash media.

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

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

**Note:**

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

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

**Note:**

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

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

---

## Before leaving the site

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

# Chapter 8: Installation verification

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

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

---

## Testing the IPSI circuit pack

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

**Note:**

With duplicated servers, use the active server.

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

---

## Testing the license file



**Important:**

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

**Note:**

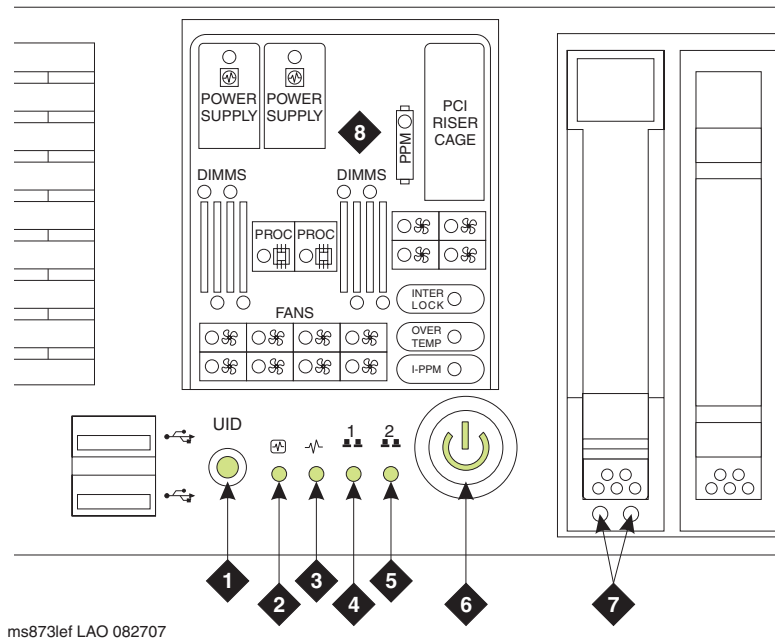
With duplicated servers, use the active server.

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

## S8730 LEDs

[Figure 7: LEDs on the front panel of the S8730 Server](#) on page 76 and [Figure 8: LEDs on the back panel of the S8730 Server](#) on page 77 show the LEDs on the S8730 Server.

**Figure 7: LEDs on the front panel of the S8730 Server**



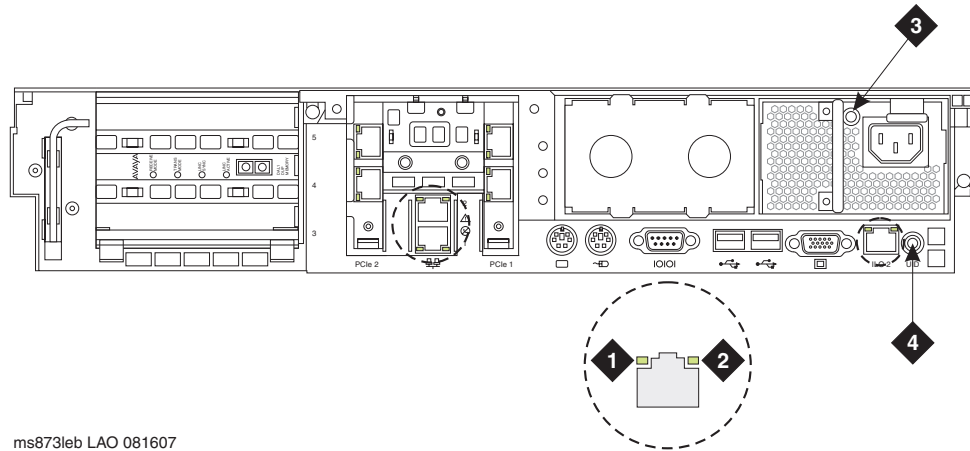
**Figure notes:**

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>1. Active/standby LED</li> <li>2. Internal health</li> <li>3. External health</li> <li>4. NIC 1 (Eth0) link/activity</li> <li>5. NIC 2 (Eth1) link/activity</li> </ul> | <ul style="list-style-type: none"> <li>6. Power on/standby button/system power. Amber means system shut down, but power still applied. Green means system on. To turn off the power, press and hold the Power button for several seconds.</li> <li>7. Hard Drive LEDs</li> <li>8. System Insight Display LEDs, which represent the system board layout.</li> </ul> |
|---|--|

**Note:**

The Active/Standby LED, which is labeled as 1 in [Figure 7](#), is on a push button. When pushed, this button has no effect other than to turn off the LED momentarily. The LED returns to the normal state within a few seconds after the button is pushed.

---

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

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

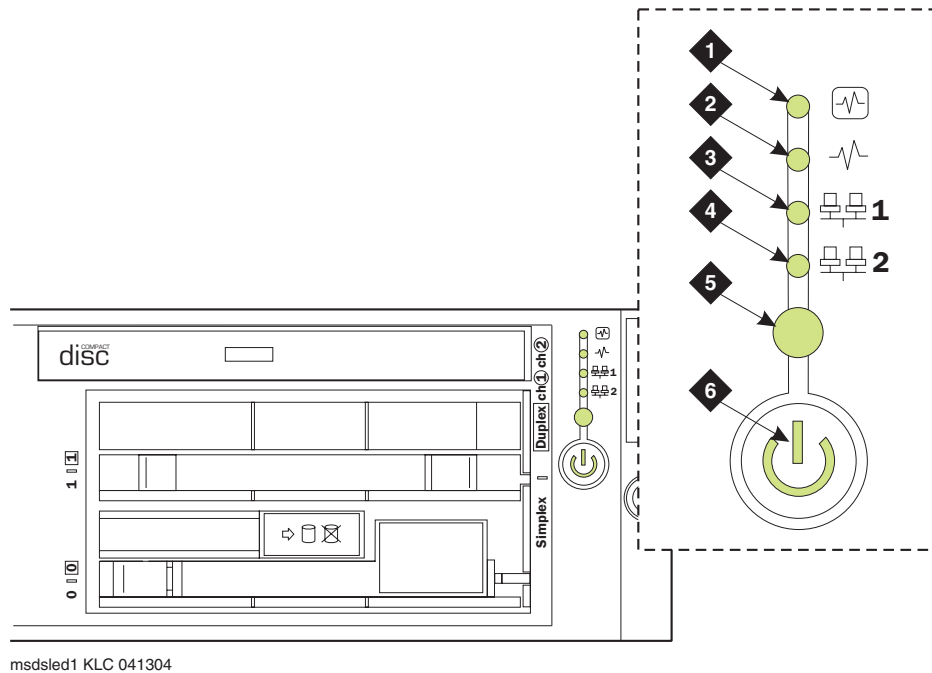
---

## S8710 and S8720 LEDs

[Figure 7: LEDs on the front panel of the S8730 Server](#) on page 76 and [Figure 8: LEDs on the back panel of the S8730 Server](#) on page 77 show the LEDs on the S8710 and the S8720 Servers.

You cannot test the LEDs on the S8710 Server.

Figure 9: LEDs on the front panel of the S8710 and the S8720 Servers



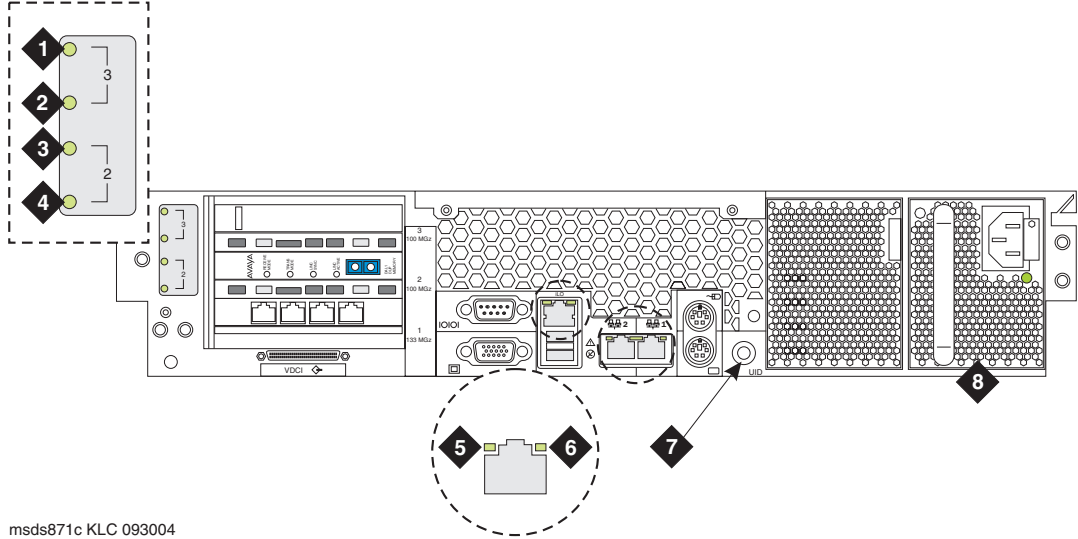
**Figure notes:**

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

**Note:**

The Active/Standby LED, which is labeled as 5 in [Figure 9](#), is on a push button. When pushed, this button has no effect other than to turn off the LED momentarily. The LED returns to the normal state within a few seconds after the button is pushed.

Figure 10: LEDs on the back panel of the S8710 and the S8720 Servers



msds871c KLC 093004

Figure notes:

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

## Additional server LED information

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

## Avaya C360 Ethernet switch LEDs

The C360 series converged, stackable, Ethernet switches include:

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

The front panel of the C360-Series switches has:

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

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

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

### System and port function LEDs on C360 Avaya Ethernet switches

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

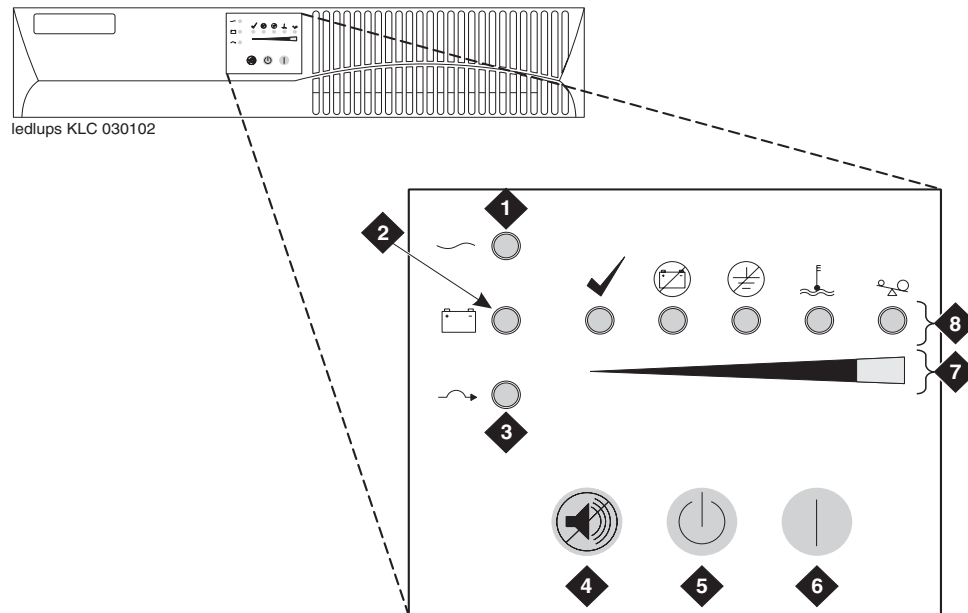


## UPS LEDs

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

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

**Figure 11: LEDs on the Powerware 9125 UPS**



**Figure notes:**

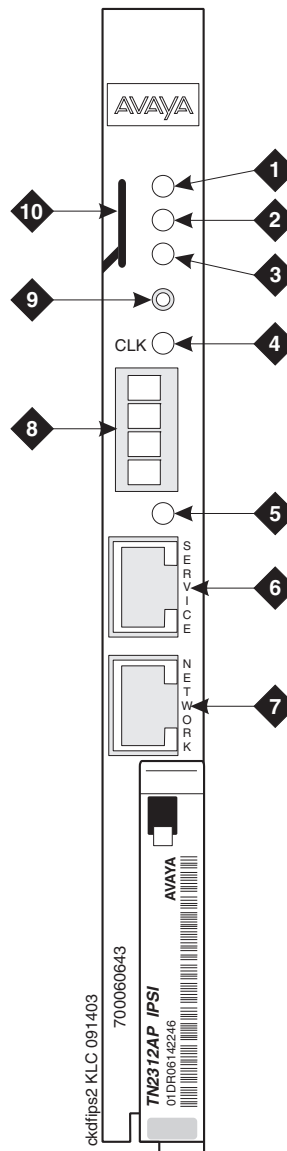
- |                            |                         |
|----------------------------|-------------------------|
| 1. Normal mode indicator   | 5. Off button           |
| 2. Battery mode indicator  | 6. On button            |
| 3. Bypass mode indicator   | 7. Bar graph indicators |
| 4. Test/Alarm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

## TN2312BP IPSI LEDs

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

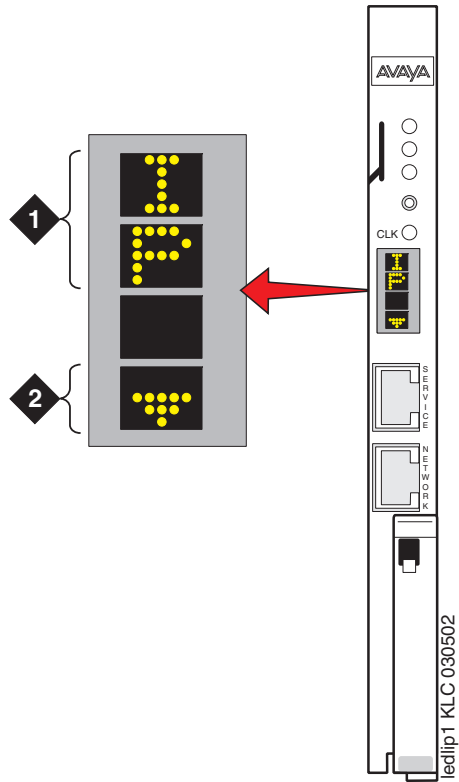
- Standard LEDs and connector slots ([Figure 12: TN2312BP IPSI circuit pack faceplate](#) on page 83)
- A programmable LED display, which indicates:
  - The type of IPSI IP address. For a dynamic address, the display shows media gateway the location of the media gateway. For a static address, the display shows I P. ([Figure 13: IPSI LED display for a static IP address](#) on page 84)
  - Connectivity

---

**Figure 12: TN2312BP IPSI circuit pack faceplate**
**Figure notes:**

- |                                   |                                    |
|-----------------------------------|------------------------------------|
| 1. Red LED                        | 6. Services RJ45 connector         |
| 2. Green LED                      | 7. Network control RJ45 connector  |
| 3. Amber LED                      | 8. Four-character LED display      |
| 4. Yellow LED (tone clock status) | 9. Pushbutton switch               |
| 5. Emergency transfer LED         | 10. Slot for the maintenance cable |
-

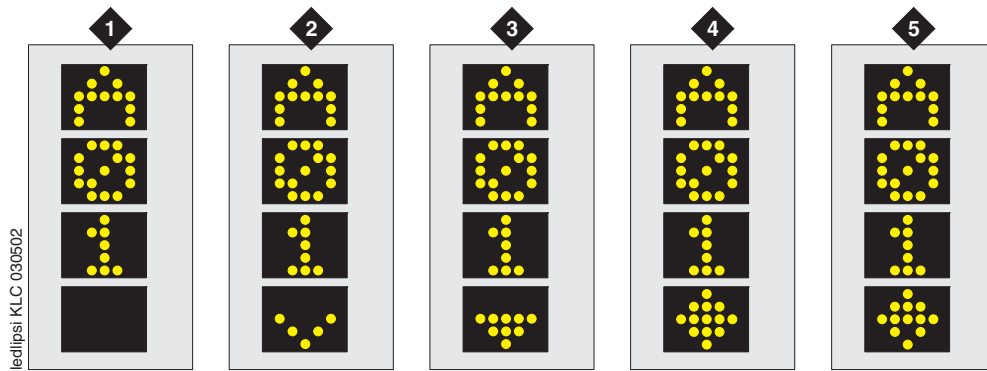
Figure 13: IPSI LED display for a static IP address



**Figure notes:**

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

Figure 14: IPSI LED display indicating connectivity status for a DHCP IP address



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



# Appendix A: Server access

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

You can access the server:

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

Steps to access a server include:

- [Connecting to the server directly](#) on page 89
- [Connecting to the server remotely over the network](#) on page 92
- [Connecting to the server remotely over a modem](#) on page 92
- [Logins for Avaya technicians and BusinessPartners](#) on page 95
- [Configuring the network for Windows 2000 and XP](#) on page 95

---

## Accessing the command line interface of the server with SSH

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

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

**Note:**

A version of PuTTY that is defaulted for SSH server access is available for Avaya Services personnel only. In this version, some values shown in the procedure below are pre-selected.

**Note:**

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

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

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

2. In the Host Name or IP address field, type **192.11.13.6** if you want to connect to the Services port. For access over the LAN or WAN, type the IP address or the host name of the server.
3. In the Port field, type **22**.
4. Under Protocol, select **SSH**.
5. In the PuTTY menu on the left, click **Connection > SSH**.
6. In the Preferred SSH protocol version field, select **2**.
7. In the Encryption options window, use the up and down arrows to set AES (SSH-2) as the top option and 3DES as the second option.

**Note:**

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

8. In the **Backspace key** area, select **Control-H**.

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

9. Click **Open**.

**Note:**

If you have not connected to this particular server before, SSH prompts you to accept the server's host key. If you save this key when prompted, you will not be prompted if you connect again later. If you do not save the key, PuTTY prompts you the next time you connect to this server.

When you connect through the interface on the Services laptop computer, if you save the host key, the host is identified as 192.11.13.6. If you later connect to a different server through the laptop interface, this new host also shows as 192.11.13.6, but it has a different key. You get a prompt in this case because it appears that the host key has changed.

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

The system displays the PuTTY window.

11. Log in as **craft**.



---

## Connecting to the server directly

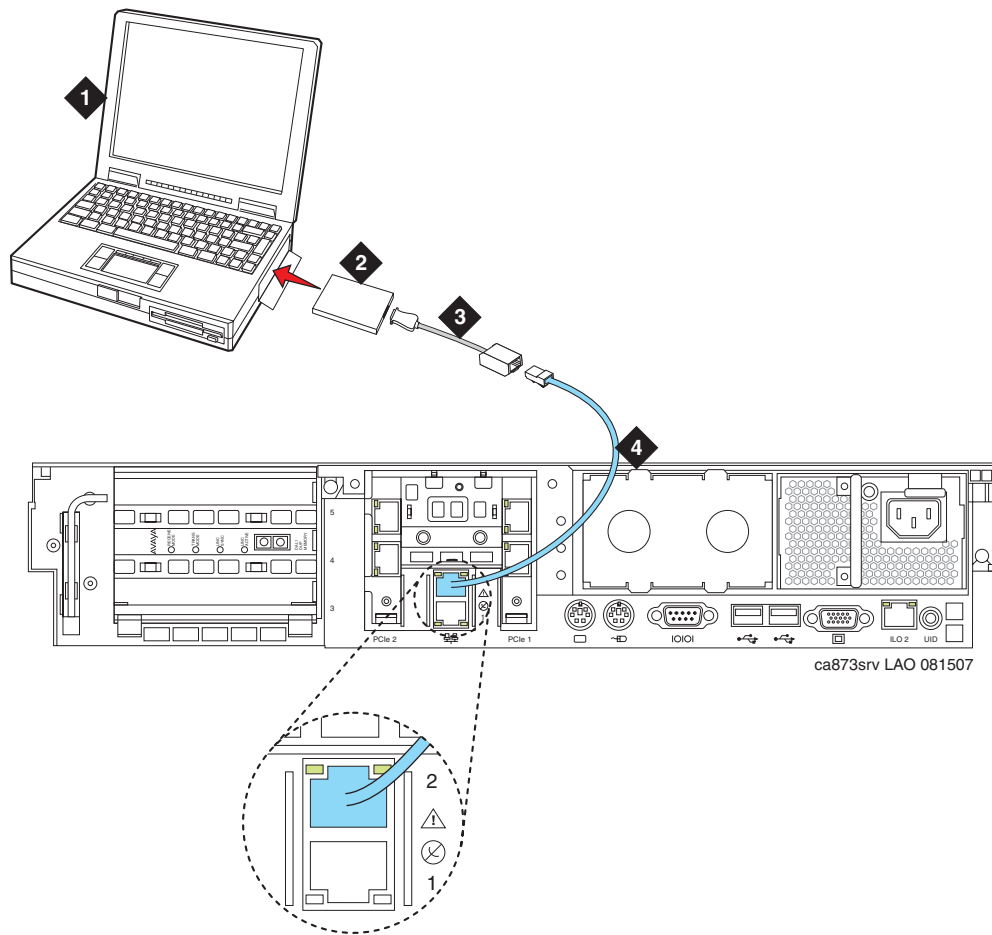
To access the server directly, use a computer with the following minimum specifications:

- A Windows 2000 or Windows XP operating system
  - 32-MB of RAM
  - 40-MB of available disk space
  - An RS-232 port connector
  - A network interface card (NIC) with a 10/100BaseT Ethernet interface
  - A 10/100 BaseT Ethernet, category 5 or better, cross-over cable with an RJ45 connector on each end (MDI to MDI-X)
  - A CD-ROM drive
1. Plug one end of the CAT5 cable into the Services access port on the back of the server. For more information, see [Figure 15: Services laptop computer connected directly to the S8730 Server](#) on page 90 or [Figure 15: Services laptop computer connected directly to the S8730 Server](#) on page 90.
  2. Plug the other end of the CAT5 cross-over cable into the NIC on your computer. Use a NIC adapter if necessary.
  3. Configure your network connection
    - IP address: 192.11.13.5
    - Subnetwork mask: 255.255.255.252

For specific information, see [Configuring the network for Windows 2000 and XP](#) on page 95.

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

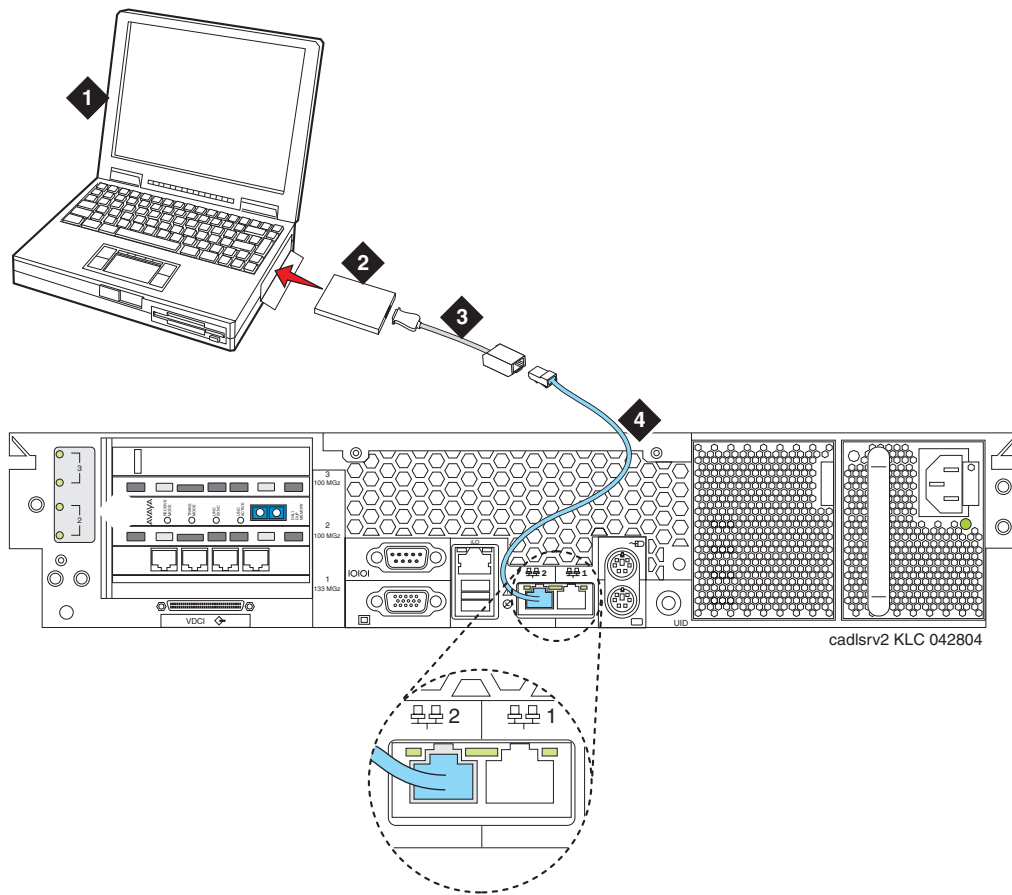
Figure 15: Services laptop computer connected directly to the S8730 Server



**Figure notes:**

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

**Figure 16: Services laptop computer connected directly to the S8710 or S8720 Server**



**Figure notes:**

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

---

## Connecting to the server remotely over the network

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

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

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

---

## Connecting to the server remotely over a modem

**Note:**

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

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

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

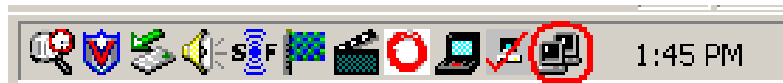
6. When the system displays the **Start PPP now** message, click **Done**. When you see the Connection Complete dialog box, your computer is connected to the server.
7. Open an SSH session using PuTTY or other client.  
See [Accessing the command line interface of the server with SSH](#) on page 87 for more information.
8. Within the SSH client, type the IP address of the active server.

---

## Finding the IP address of the active server

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

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



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

---

## Accessing the Maintenance Web Interface

You can administer the server through the Maintenance Web Interface. Access the Maintenance Web Interface when connected:

- Over the customer network with MS Internet Explorer 5.5 or 6.0.
- Directly to the Services port on the server. For more information, see [Figure 15: Services laptop computer connected directly to the S8730 Server](#) on page 90 or [Figure 15: Services laptop computer connected directly to the S8730 Server](#) on page 90.

To access the Maintenance Web Interface, you must first bypass any proxy servers.

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

## Appendix A: Server access

6. Open the MS Internet Explorer Web browser to access the Maintenance Web Interface.
  - If you are connected directly, in the **Address** field, type **192 . 11 . 13 . 6**.
  - If you are connected remotely through a modem, in the **Address** field, type in the IP address or the DNS host name of the server.

**Note:**

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

7. When prompted, log in.
8. When you see a message that asks **Do you want to suppress alarms?**, select **Yes**.
9. Click **Launch Maintenance Web Interface**.

---

## Using the SAT command line prompt

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

| Type of connection                | Procedure  |
|-----------------------------------|--|
| Using SAT with SSH:               | See <a href="#">Accessing the command line interface of the server with SSH</a> on page 87.  |
| Using SAT with Terminal Emulation | <p>To use a command line interface in a terminal emulation window, open your terminal emulation application. Configure the terminal emulation program port settings as follows:</p> <ul style="list-style-type: none"><li>● Speed: 115200 baud or 9600 baud if you use a serial modem connection</li><li>● No parity</li><li>● 8 data bits</li><li>● 1 stop bit</li><li>● No flow control</li></ul> <p>NOTE: Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are the only terminal emulation programs that Avaya supports.</p> <p>Use either the IP address or the DNS host name to establish a network connection to the <i>active</i> server. Use port <b>5023</b> for this connection. Use SAT commands on the active server only. When prompted, log in to the server as <b>craft</b>.</p> |

---

## Logins for Avaya technicians and BusinessPartners

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

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

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

---

## Configuring the network for Windows 2000 and XP



### Important:

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

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

Windows 2000 or Windows XP should automatically detect the Ethernet card in your system and create a LAN connection. More than one connection might appear.

2. Right-click on the correct **Local Area Connection** and left-click **Properties** to display the Local Area Connection Properties dialog box.
3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties** to display the Internet Protocol (TCP/IP) Properties dialog box.
5. On the General tab, select **Use the following IP address**.
6. Make a note of any IP addresses or other entries that you have to clear. You might need to restore them later to connect to another network

Enter the following:

- IP address: 192 . 11 . 13 . 5
- Subnet mask: 255 . 255 . 255 . 252

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

---

## Setting the browser options for Internet Explorer 6.0

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

To set browser options for Internet Explorer 6.0:

1. In Internet Explorer 6.0, click **Tools > Internet Options**.
2. Select the **Connection** tab.
3. Click on **LAN settings**, then **Advanced**.
4. In the **Do not use proxy server for addresses beginning with** field, type the IP address for each server you intend to access remotely.  
  
If the IP addresses have the first or first and second octets the same, you can shorten the addresses to xxx.xxx.\* (example, 135.9.\*).
5. Click **OK** to close each dialog box.



# Appendix B: Installation troubleshooting

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

- [Troubleshooting the installation of the server hardware](#) on page 97
- [Troubleshooting the configuration of the server hardware](#) on page 98
- [Troubleshooting the installation of the license file and the Avaya authentication file](#) on page 100

---

## Troubleshooting the installation of the server hardware

| Problem                         | Possible solution  |
|---------------------------------|--|
| No power to the UPS             | <ul style="list-style-type: none"><li>● Ensure that the UPS is plugged into the outlet.</li><li>● Ensure that the outlet has power.</li><li>● For other solutions, see the user guide for the UPS.</li></ul>   |
| No power to the Ethernet switch | <ul style="list-style-type: none"><li>● Ensure that the Ethernet switch is plugged into the UPS or the outlet.</li><li>● Ensure that the UPS or outlet has power.</li><li>● For other solutions, see the user guide for the Ethernet switch.</li></ul>   |
| No power to the server          | <ul style="list-style-type: none"><li>● Ensure that the server is plugged into the UPS.</li><li>● Ensure that the UPS has power.</li><li>● Push the power button on the front of the server.</li></ul>   |
| The servers are not shadowing   | <ul style="list-style-type: none"><li>● Make sure you are using a cross-over cable.</li><li>● Make sure fiber optic cable is plugged in correctly, RX to TX and TX to RX.</li></ul>  |
| The IPSI LEDs flash             | <ul style="list-style-type: none"><li>● Ensure that the IPSI is in the correct slot. Use slot 1 for the G650 Media Gateway, slot 2 for the G600 Media Gateway, and the Tone-Clock slot for all others.</li><li>● Ping the IPSI from server.</li><li>● Ping the server from the IPSI.</li></ul> |
|                                 |  |

## Troubleshooting the configuration of the server hardware

### Troubleshooting the configuration of the server hardware

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

Troubleshooting the configuration of the server hardware (continued)

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

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

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

# Index

---

## Numerical

8730 Server configurations . . . . . [13](#)

---

## A

access server  
     directly . . . . . [89](#)  
     remotely over modem . . . . . [92](#)  
     remotely over network . . . . . [92](#)  
 accessing Maintenance Web Interface . . . . . [93](#)  
 accessing the server . . . . . [32](#)  
 add  
     IP interface information . . . . . [54](#)  
     media gateways . . . . . [52](#)  
 administer  
     IPSI circuit pack . . . . . [57](#)  
 AIW. See Avaya Installation Wizard  
 alarm activation level  
     setting . . . . . [55](#)  
 alarms  
     enabling to INADS via SNMP . . . . . [73](#)  
     setting selected traps . . . . . [26](#)  
     to INADS by way of modem, enabling . . . . . [72](#)  
     viewing. . . . . [71](#)  
 ARP cache, clearing . . . . . [31](#)  
 Avaya Installation Wizard, using . . . . . [37](#), [41](#)

---

## B

backing up files to compact flash . . . . . [73](#)

---

## C

C363T or C364T Ethernet switch  
     configuring . . . . . [27](#)  
     LEDs . . . . . [80](#)  
     security alert . . . . . [27](#)  
 clearing ARP cache . . . . . [31](#)  
 collocated servers, connecting to . . . . . [19](#)  
 command line interface. . . . . [94](#)  
 Communication Manager  
     installing software. . . . . [31](#)  
 compact flash, backing up to . . . . . [73](#)  
 configure  
     Avaya C363T or C364T Ethernet switch . . . . . [27](#)  
     media server 2 . . . . . [48](#)

    modem . . . . . [43](#)  
     network interface card (NIC) . . . . . [47](#)  
     server . . . . . [35](#), [51](#)  
     UPS . . . . . [23](#)  
 connect to customer network . . . . . [13](#)  
 connection to LAN, verifying. . . . . [42](#)  
 copy files to server . . . . . [36](#)  
 customer network, connecting to . . . . . [13](#)

---

## D

date and time, verifying . . . . . [70](#)  
 daylight savings rules  
     location . . . . . [69](#)  
     setting . . . . . [68](#)  
 DHCP IP addressing  
     IPSI circuit pack . . . . . [57](#)  
     using . . . . . [62](#)  
 diffserv parameters, setting . . . . . [61](#)  
 direct access to server . . . . . [89](#)  
 disable unused Ethernet switch ports . . . . . [71](#)  
 disconnecting from server. . . . . [48](#)  
 duplicated IPSIs, enabling. . . . . [55](#)

---

## E

enable Ethernet switch ports . . . . . [71](#)  
 ESS compatibility. . . . . [45](#)  
 Ethernet interface assignments . . . . . [40](#)  
 Ethernet switch  
     configuring . . . . . [29](#)  
     default IP addresses. . . . . [27](#)  
     disabling unused ports. . . . . [71](#)  
     preparing to configure . . . . . [28](#)  
 Extra Large configuration . . . . . [45](#)

---

## F

faceplate  
     TN2312BP circuit pack . . . . . [82](#)  
 firewall settings. . . . . [46](#)

---

## I

INADS  
     enabling alarms to by way of modem . . . . . [72](#)  
 inputting translations . . . . . [51](#)  
 installation

## Index

|  |                        |
|--|------------------------|
| troubleshooting . . . . .                | <a href="#">97</a>     |
| using the Wizard . . . . .               | <a href="#">37, 41</a> |
| installing                               |                        |
| Communication Manager software . . . . . | <a href="#">33</a>     |
| translation file . . . . .               | <a href="#">55</a>     |
| interchanging servers . . . . .          | <a href="#">49</a>     |
| IP address                               |                        |
| finding for the active server . . . . .  | <a href="#">93</a>     |
| set static . . . . .                     | <a href="#">58</a>     |
| use DHCP . . . . .                       | <a href="#">62</a>     |
| IP address, set static. . . . .          | <a href="#">58</a>     |
| IP interface                             |                        |
| enabling control . . . . .               | <a href="#">65</a>     |
| upgrading firmware version . . . . .     | <a href="#">65</a>     |
| verify translations . . . . .            | <a href="#">65</a>     |
| IP interface information                 |                        |
| adding to translations . . . . .         | <a href="#">54</a>     |
| IPSI                                     |                        |
| connecting to . . . . .                  | <a href="#">57</a>     |
| enabling duplication. . . . .            | <a href="#">55</a>     |
| LEDs . . . . .                           | <a href="#">82</a>     |
| program switch ID and cabinet. . . . .   | <a href="#">57</a>     |

---

## L

|                                      |                    |
|--------------------------------------|--------------------|
| LED                                  |                    |
| additional information . . . . .     | <a href="#">79</a> |
| LEDs                                 |                    |
| Avaya Ethernet switches . . . . .    | <a href="#">80</a> |
| IPSI . . . . .                       | <a href="#">82</a> |
| S8700-series Server . . . . .        | <a href="#">77</a> |
| S8730 Server. . . . .                | <a href="#">76</a> |
| UPS . . . . .                        | <a href="#">81</a> |
| license file, testing . . . . .      | <a href="#">75</a> |
| license, verifying status. . . . .   | <a href="#">66</a> |
| location                             |                    |
| setting for media gateways . . . . . | <a href="#">69</a> |
| login, super-user. . . . .           | <a href="#">36</a> |
| LSP compatibility . . . . .          | <a href="#">45</a> |

---

## M

|  |                    |
|--|--------------------|
| Maintenance Web Interface, accessing . . . . . | <a href="#">93</a> |
| manual configuration                           |                    |
| configuration, manual method . . . . .         | <a href="#">37</a> |
| media gateways, adding . . . . .               | <a href="#">52</a> |
| media server                                   |                    |
| applying power . . . . .                       | <a href="#">32</a> |
| media server 2                                 |                    |
| configuring . . . . .                          | <a href="#">48</a> |
| modem  |                    |
| access to server . . . . .                     | <a href="#">92</a> |
| configuring . . . . .                          | <a href="#">43</a> |
| connect to server . . . . .                    | <a href="#">19</a> |
| modem options, setting. . . . .                | <a href="#">20</a> |

|   |                    |
|---|--------------------|
| modem, enabling alarms to INADS . . . . . | <a href="#">72</a> |
|---|--------------------|

---

## N

|   |                    |
|---|--------------------|
| network interface card (NIC)                  |                    |
| configuring . . . . .                         | <a href="#">47</a> |
| network time server (NTP), enabling . . . . . | <a href="#">46</a> |

---

## P

|   |                    |
|---|--------------------|
| PNC license settings for S8700 . . . . .                  | <a href="#">9</a>  |
| post installation tasks . . . . .                         | <a href="#">74</a> |
| power   |                    |
| applying to media server . . . . .                        | <a href="#">32</a> |
| pre-installation tasks at the installation site . . . . . | <a href="#">9</a>  |
| Processor Ethernet . . . . .                              | <a href="#">20</a> |
| PuTTY, SSH client . . . . .                               | <a href="#">87</a> |

---

## R

|                                      |                    |
|--------------------------------------|--------------------|
| RAID level 1 (S8730 server). . . . . | <a href="#">13</a> |
| remote access to server              |                    |
| over modem . . . . .                 | <a href="#">92</a> |
| over network . . . . .               | <a href="#">92</a> |

---

## S

|   |                        |
|---|------------------------|
| S8700   |                        |
| active server, finding the IP address . . . . . | <a href="#">93</a>     |
| port connections. . . . .                       | <a href="#">14</a>     |
| S8700-series Media Server                       |                        |
| PNC license settings . . . . .                  | <a href="#">9</a>      |
| S8700-series Server                             |                        |
| LEDs . . . . .                                  | <a href="#">77</a>     |
| S8730 Server                                    |                        |
| LEDs . . . . .                                  | <a href="#">76</a>     |
| saving translations . . . . .                   | <a href="#">51, 55</a> |
| separated servers, connecting to                |                        |
| server  |                        |
| accessing. . . . .                              | <a href="#">32</a>     |
| configuring . . . . .                           | <a href="#">35, 51</a> |
| copying files to . . . . .                      | <a href="#">36</a>     |
| disconnecting from . . . . .                    | <a href="#">48</a>     |
| LED, additional information . . . . .           | <a href="#">79</a>     |
| LEDs . . . . .                                  | <a href="#">76, 77</a> |
| verify connectivity . . . . .                   | <a href="#">65</a>     |
| verifying LAN connection. . . . .               | <a href="#">42</a>     |
| server configuration, manual method. . . . .    | <a href="#">37</a>     |
| set   |                        |
| alarm activation level . . . . .                | <a href="#">55</a>     |
| daylight savings rules . . . . .                | <a href="#">68</a>     |
| selected traps (alarming). . . . .              | <a href="#">26</a>     |
| static IP address . . . . .                     | <a href="#">58</a>     |
| set static IP address . . . . .                 | <a href="#">58</a>     |

|  |                    |
|--|--------------------|
| SNMP   |                    |
| preparing to configure . . . . .                     | <a href="#">25</a> |
| SNMP modules   |                    |
| administering . . . . .                              | <a href="#">26</a> |
| software, installing Communication Manager . . . . . | <a href="#">33</a> |
| spanning tree  |                    |
| enabling . . . . .                                   | <a href="#">29</a> |
| setting version . . . . .                            | <a href="#">29</a> |
| SSH  |                    |
| about . . . . .                                      | <a href="#">21</a> |
| access with. . . . .                                 | <a href="#">87</a> |
| static IP addressing                                 |                    |
| IPSI circuit pack . . . . .                          | <a href="#">57</a> |
| setting . . . . .                                    | <a href="#">58</a> |
| static IP addressing, setting. . . . .               | <a href="#">58</a> |
| super-user login . . . . .                           | <a href="#">36</a> |

---

## T

|  |   |
|--|---|
| Telnet   |   |
| configuring for Win2000/XP . . . . .           | <a href="#">32</a>                      |
| terminal emulation . . . . .                   | <a href="#">94</a>                      |
| testing  |   |
| license file . . . . .                         | <a href="#">75</a>                      |
| server installation . . . . .                  | <a href="#">75</a>                      |
| TN2312BP . . . . .                             | <a href="#">75</a>                      |
| TN2312BP                                       |   |
| faceplate . . . . .                            | <a href="#">82</a>                      |
| LEDs . . . . .                                 | <a href="#">82</a>                      |
| program switch ID and cabinet. . . . .         | <a href="#">57</a>                      |
| TN2312BP, testing. . . . .                     | <a href="#">75</a>                      |
| translation file                               |   |
| installing . . . . .                           | <a href="#">55</a>                      |
| translations                                   |   |
| inputting . . . . .                            | <a href="#">51</a>                      |
| IP interface. . . . .                          | <a href="#">51</a>                      |
| saving . . . . .                               | <a href="#">51</a> , <a href="#">55</a> |
| verifying . . . . .                            | <a href="#">67</a>                      |
| troubleshooting, server installation . . . . . | <a href="#">97</a>                      |

---

## U

|  |                    |
|--|--------------------|
| upgrading                                |                    |
| IP interface firmware version . . . . .  | <a href="#">65</a> |
| UPS                                      |                    |
| default IP addresses for S8700 . . . . . | <a href="#">24</a> |
| LEDs . . . . .                           | <a href="#">81</a> |
| security alert . . . . .                 | <a href="#">23</a> |
| SNMP module . . . . .                    | <a href="#">23</a> |
| UPS, configuring. . . . .                | <a href="#">23</a> |
| using DHCP IP address . . . . .          | <a href="#">62</a> |
| using this documentation . . . . .       | <a href="#">8</a>  |

---

## V

|                                    |                    |
|------------------------------------|--------------------|
| verify                             |                    |
| connectivity to servers . . . . .  | <a href="#">65</a> |
| date and time . . . . .            | <a href="#">70</a> |
| IP interface translated . . . . .  | <a href="#">65</a> |
| license status . . . . .           | <a href="#">66</a> |
| server connection to LAN . . . . . | <a href="#">42</a> |
| translations . . . . .             | <a href="#">67</a> |
| view alarms . . . . .              | <a href="#">71</a> |
| VLAN parameters, setting. . . . .  | <a href="#">61</a> |

---

## W

|                                |   |
|--------------------------------|---|
| Wizard, installation . . . . . | <a href="#">37</a> , <a href="#">41</a> |
|--------------------------------|---|

