Implementing Avaya Aura® Communication Manager Solution

Release 6.2
03-603559
Issue 2
December 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

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

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format

US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

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

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

CE

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

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

European Union Battery Directive

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

Japan

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

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

If this is a Class A device:

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

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

If this is a Class B device:

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

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

The purpose of this document is to provide the information, references, and procedures to Avaya partners and customer administrators who will install Communication Manager, and perform initial administration, to set up an enterprise telephony application.

Checklist for setting up Communication Manager

The following tasks help in setting up Communication Manager for an enterprise telephony application:

#	Task	Reference	
1	Installing UPS in rack, if purchased from Avaya	Mounting UPS brackets on page 16	
2	Configuring SNMP on UPS	Installing the SNMP module in the UPS on page 15	
3	• Installing S8800 in rack • Installing the HP DL360 G7 Server • Installing the Dell™ PowerEdge™ R610 Server	• *Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603444 • *Installing the HP DL360 G7 Server*, 03-603799 • *Installing the Dell™ PowerEdge™ R610 Server*, 03-603793	
4	Implementing Communication Manager	*Implementing Avaya Aura® Communication Manager*, 03-603558	
5	Installing and configuring port networks, if being used	*Installing the Avaya G650 Media Gateway*, 03-300685	

#	Task	Reference	
6	Installing and administering Branch Gateways, if being used	• *Quick Start for Hardware Installation: Avaya G430 Branch Gateway, 03-603236* • *Quick Start for Hardware Installation: Avaya G450 Branch Gateway, 03-602053*	
7	Administering IPSIs	This document	
8	Verifying installation	This document	
9	Completing post-installation tasks	This document	

Note:

This document provides an overview of the Communication Manager administration tasks. For more information on administering Communication Manager, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Prerequisites

About this task

Before you use this document, ensure you fulfill the following prerequisites:

Procedure

1. Installation and administration documents of the servers, gateways, and Communication Manager are available for reference
2. Required data such as IP addresses to allocate to the servers and gateways are ready on the worksheets
3. Necessary enterprise and purchase information is registered with Avaya at least two weeks in advance
4. Avaya has sent license and system ID information that is necessary for Communication Manager administration
5. Communication Manager template is installed to enter initial system translations

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			
03-603793	*Installing the Dell™ PowerEdge™ R610 Server*	Describes the steps to install the Dell R610 server.	Implementation Engineers, Support Personnel
03-603799	*Installing the HP ProLiant DL360 G7 Server*	Describes the steps to install the HP DL360 G7 server.	Implementation Engineers, Support Personnel
03-603444	*Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*	Describes the steps to install the S8800 server.	Implementation Engineers, Support Personnel
Maintenance and Troubleshooting			
03-603446	*Maintaining the Avaya S8800 Server for Avaya Aura® Communication Manager*	Describes the steps to maintain the Avaya S8800 server.	Implementation Engineers, Support Personnel
03-603804	*Maintaining and Troubleshooting the Dell™ PowerEdge™ R610 Server*	Describes the steps to maintain and troubleshoot the Dell server.	Implementation Engineers, Support Personnel
03-603803	*Maintaining and Troubleshooting the HP ProLiant DL360 G7 Server*	Describes the steps to maintain and troubleshoot the HP server.	Implementation Engineers, Support Personnel
Administration			

Document number	Title	Description	Audience
555-233-504	*Administering Avaya Aura® Communication Manager*	Describes procedures to administer Communication Manager.	Implementation Engineers, Support Personnel

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In

addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Installing UPS

Installing the SNMP module in the UPS

About this task

The following image helps you to install the SNMP module in the UPS.

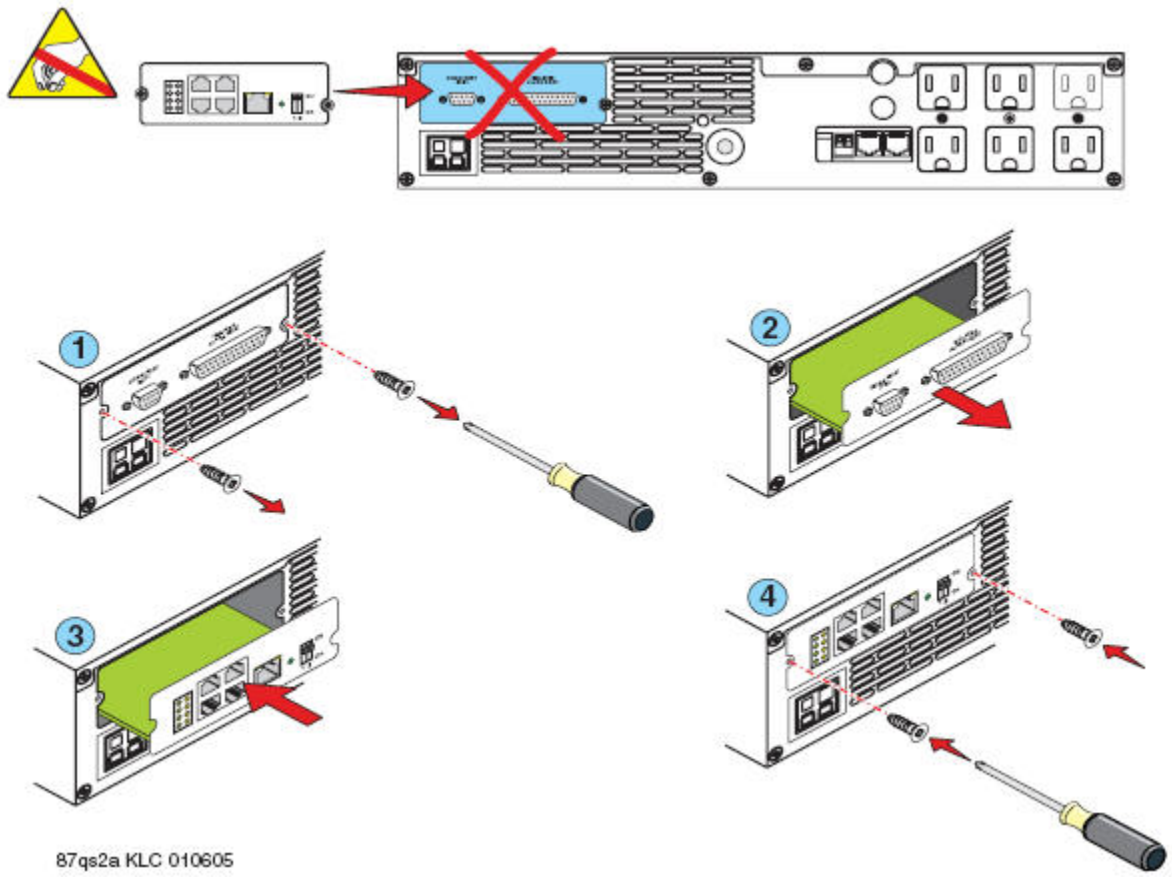

Figure 1: Steps to install the SNMP module in the UPS

UPS brackets

About this task

The following image helps you to mount the UPS brackets.

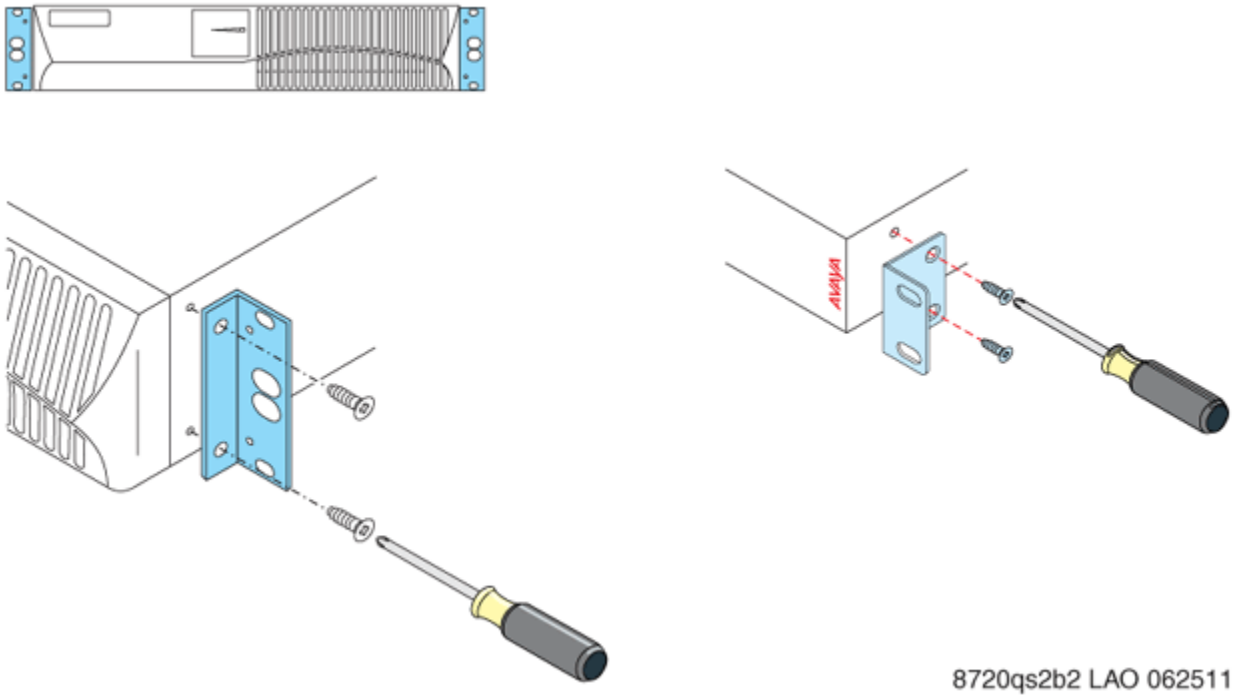

Figure 2: UPS mounting brackets

Chapter 3: SNMP configuration

Configuring SNMP modules in the UPS

About this task

You can use this procedure to configure the SNMP module in the USP 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.

Note:

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

Important:

This procedure apply only to an Avaya supplied uninterruptible power supply (UPS) with a Simple Network Management Protocol (SNMP) module. Do not use this procedure to set traps on a UPS that Avaya does not supply. For information on how to configure a UPS device that Avaya has not supplied, see the manual that the UPS manufacturing company supplies with the UPS device.

Procedure

1. For the SNMP module to properly report alarms, configure a unique IP address for the UPS on the SNMP module and the server.
2. To configure an IP address for the UPS, configure either the default IP address from Avaya or the IP address the customer provides. Configure the following parameters:
   - IP address
   - Subnet mask
   - Gateway IP address
   - Trap receiver IP address
   - Community string (get, set, trap)

Default IP addresses for the UPS

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

Parameter	IP Address
IP address for the UPS	198.152.254.239
Gateway address for the UPS	198.152.254.201
IP address for the trap receiver (server)	Customer provided

For more information about how to administer the SNMP module in the UPS, see *Administering the SNMP module*.

Prerequisites for administering the SNMP module

Procedure

1. Plug your Services laptop computer into the correct administration port on the SNMP module on the UPS.
2. Plug the UPS into a nonswitched electrical outlet.
3. Ensure 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:

   Native Configuration Manager is an Avaya supported terminal emulation application.
4. If you use a Network Management System (NMS) to monitor the UPS, coordinate the assignment of community names with the network administrator. If you do not use an NMS, 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 more information about which traps to set, see *Recommended trap settings*.

5. If the control network is nondedicated, ensure that the 162/udp port for input to server is enabled and the default port is disabled. If you do not enable the 162/udp port and disable the default port, the server cannot receive the traps from either UPS.

Administering the SNMP module

Procedure

1. Connect the RS-232 serial port of your Services laptop computer to the DB-9 connector on the back of the SNMP module for UPS1. Use the DB-9 to DB-9 serial cable that is supplied with the SNMP module.
2. Open a VT-100 terminal emulation session on your computer.
3. Set the IP address for the UPS.

   Note:

   Use the default IP addresses.
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 more information on which traps to set, see *Recommended trap settings*.
8. When you finish, disconnect your computer from the UPS.
9. Connect one end of a CAT5 straight-through cable to the RJ45 connector on the UPS SNMP module.

   For more information on connectivity, see the quick start guide on hardware installation of your server.

Recommended trap settings

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 Avaya supplies.

Chapter 4: IP inteface configuration

Connecting to the IPSIs

About this task

Connect CAT5 cables from the IPSI circuit packs to the customer LAN.

Configuration of IPSI address configuration

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.

Note:

If the laptop's IP address and mask are not 192.168.13.5 and 255.255.255.0 respectively, you cannot connect the laptop to the IPSI.

Connecting the laptop directly to the IPSI

About this task

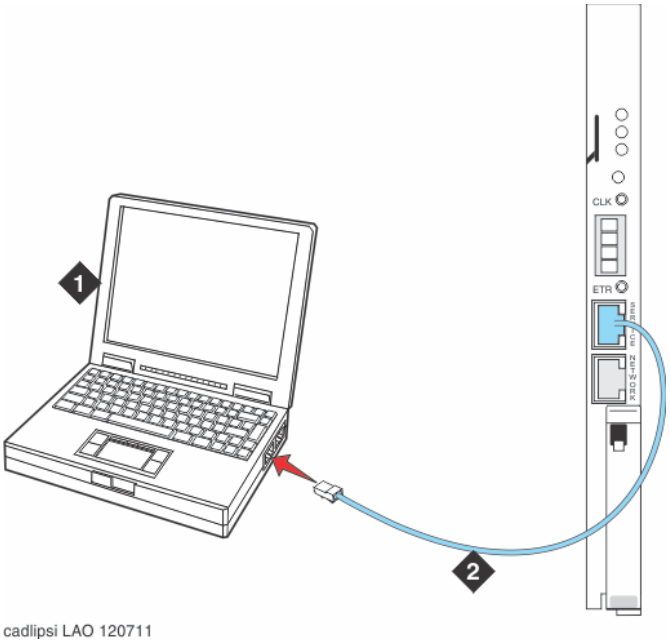

Figure 3: Connecting the laptop directly to the IPSI

Table 1: Connecting the laptop directly to the IPSI

Number	Description
1	Services laptop computer
2	CAT5 crossover cable to IPSI

Configuring IPSI address configuration

Procedure

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

Note:

While connected to the IPSI, type **help** or **?** to obtain online help. Most commands have two-letter 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.
8. Type **show port 1** and press Enter.

   The system displays the current control interface settings.

9. 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]:
```

10. Type **quit** and press Enterto save the changes and exit the IPSI session.
11. Log back in to the IPSI using SSH.
12. Type **show control interface** and press Enter.

    The system displays the IP address, subnet mask, and default gateway information. Verify that the information you entered was accurate.

13. 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.
14. Type **quit** and press Enterto save the changes and exit the IPSI session.
15. Log back in to the IPSI using SSH.
16. Use **show control interface** to verify the administration.
17. Type **exit** and press Enter.

Setting the VLAN and diffserv parameters

Procedure

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 following **set** commands 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:

   Ensure that the settings for these parameters on the IPSIs are consistent with the settings on the servers and other network devices.

   - **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 IPSI faceplate.
8. Check the LED on the IPSI faceplate. Verify that the display shows the letters I and P and a filled-in V at the bottom. See the *IPSI LED display for static address* section.

   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.

IPSI LED display for static address

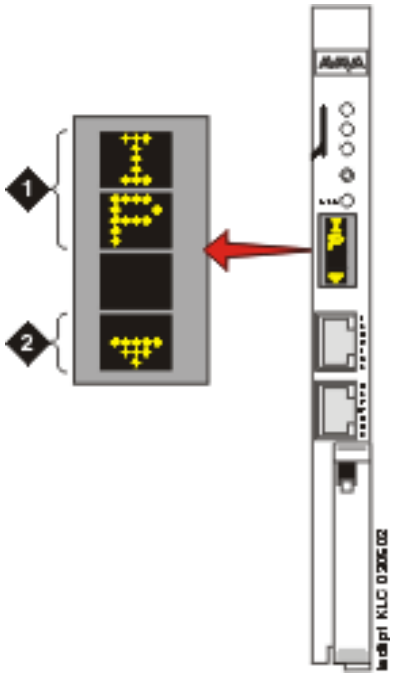

Figure 4: IPSI LED display for static address

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

Chapter 5: IP interface translations

Entering initial system translations

Before you begin

You can prepare the initial translations offsite and save the translations in the translation file. You must store the translation file in the `/etc/opt/defty` directory with *xln1* and *xln2* names. You can also save the full backup of a system in a translation file and then you can restore the files on another system.

Procedure

1. Open a SAT session.
2. Log in as the root user.
3. If the system translations were prepared offsite, install the prepared translations and reset Communication Manager using the SAT command **`reset system 4`** or **`drestart 1 4`** on Secure Shell (SSH).
4. If translations were not prepared offsite, enter minimal translations to verify connectivity to the port networks.
5. After you enter the translations, type **`save translation`** and press `Enter` to save the translations to the hard disk drive.
6. Type **`reset system 4`** or **`drestart 1 4`** and press `Enter` to enable the software to read the copied translations.

Adding media gateways

Procedure

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.

Note:

If you loaded system translations on the server, do not add media gateways to administer the IPSI.

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
                 Location: 1         IP Network Region: 1
Rack:                 Room:              Floor:             Building:
 CARRIER DESCRIPTION
   Carrier       Carrier Type        Number
      E        not-used             PN 01
      D        not-used             PN 01
      C        not-used             PN 01
      B        not-used             PN 01
      A        G650-port            PN 01
```

Enabling the IPSI

Procedure

1. Type **change system-parameters ipserver-interface** and press Enter.
2. On the IP Server Interface System Parameters screen, verify that the primary control subnetwork address is correct.

```
change system-parameters ipserver-interface                    Page   1
of   1
IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS
SERVER INFORMATION
Primary Control Subnet Address:                                      *
Secondary Control Subnet Address:                                    *
OPTIONS
Switch Identifier: A
IPSI Control of Port Networks: enabled
A-side IPSI Preference: enabled
IPSI Socket Sanity Timeout: 3
QoS PARAMETERS
802.1p: 6
DiffServ: 46
         NOTE: * indicates data changed on the Server
```

3. On a duplicated server, the system displays the following screen. Verify that the primary control and the secondary control subnetwork addresses are correct.

   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. Use the Network Configuration option on the System Management Interface to see the IP address of the server.

```
change system-parameters ipserver-interface                    Page   1
of   1
IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS
SERVER INFORMATION
Primary Control Subnet Address: 10.13.0.0
Secondary Control Subnet Address:
OPTIONS
Switch Identifier: init@svs8730-1-srv1>
IPSI Control of Port Networks: enabled
A-side IPSI Preference: enabled
IPSI Socket Sanity Timeout: 3
QoS PARAMETERS
802.1p: 6
DiffServ: 46
```

4. If the information in the **Control Subnet Address** field is incorrect, use System Management Interface to change the server configuration to match the Server IP address in the Network Configuration option. Then return to this procedure.
5. If the information in the **Primary Control Subnet Address** field, the **Secondary Control Subnet Address** field, or both fields is incorrect, use the System Management 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.
6. Set the **Switch Identifier** field to the switch ID letter. Acceptable switch ID letters are A through J. The default setting is A.
7. Set the **IPSI Control of Port Networks** field to **enabled**.
8. Press `Enter` to save the changes.

Adding the IPSI to the system

Procedure

1. Type **`add ipserver-interface PNnumber`** and press `Enter`.

   The system displays the IP Server Interface Administration - Port Network screen.
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 8                                        Page
1 of   1
          IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 8
   IP Control? y           Ignore Connectivity in Server Arbitration?
n
   Encryption? y
 PRIMARY IPSI                                 QoS AND ETHERNET SETTINGS
        DHCP? n                    Use System Level Parameter Values? y
                                                          802.1p: 6
    Location:  5AXX                                     DiffServ: 46
  Subnet Mask: /24                                           Auto? y
   IP Address:
      Gateway:
 SECONDARY IPSI                               QoS AND ETHERNET SETTINGS
        DHCP? n                    Use System Level Parameter Values? y
                                                          802.1p: 6
    Location:  5B01                                     DiffServ: 46
  Subnet Mask: /24                                           Auto? y
   IP Address:
      Gateway:
```

3. In the **Host** field, type the IP address of the IPSI that is listed in the **Location** field.

```
add ipserver-interface 8
          IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 3
IP Control? y                         Ignore Connectivity in Server
Arbitration? n
Encryption? n
 PRIMARY IPSI                                 QoS AND ETHERNET SETTINGS
     Location: 3A01                        Use System Level Parameter
Values? y   Subnet Mask: /24
802.1p: 6
   IP Address:                                                DiffServ: 46
      Gateway:                                                      Auto?
y
```

4. Set the **IP Control** field to y.
5. Verify that all the other fields are populated and submit the screen to save the changes.
6. Repeat this procedure for each port network.

Enabling IPSI duplication for duplicated control network only

Before you begin

Port networks with duplicated IPSIs have both primary and secondary IPSI circuit packs. To disable IPSI duplication, ensure that all primary IPSI circuit packs are active.

Procedure

1. On the SAT screen, type **`change system-parameters duplication`** and press **Enter**.
2. In the **Enable Operation of IPSI Duplication** field, type `y`.
3. Save the changes.

Setting the alarm activation level

Procedure

1. On the SAT screen, 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. Press `Enter` to save the changes.

Saving translations

Procedure

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

Verifying connectivity to the server

Procedure

1. Log in to Communication Manager System Management Interface as craft.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Ping**.

4. Click one of the following options for the **Endpoints to Ping** field:
   - **Host Name Or IP address**: To ping a computer of the specified IP address or the host name.
   - **IPSI's with cab number (1~99)**: To ping the specified IPSI.
   - **Other server via duplication link**: To ping the other server.
5. Click **Do not look up symbolic names for host addresses**, if required.
6. Click **Bypass normal routing tables and send directly to a host**, if required.
7. Click **Execute Ping**.
8. Verify that all endpoints respond correctly.

Verifying that the IPSIs are translated

Procedure

1. On the SAT screen (SSH connection) , type `list ipserver-interface`, and press **Enter**.
2. Verify that all IPSI circuit packs are translated.

Upgrading the IPSI firmware version (if necessary)

Before you begin

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

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)** > **IPSI Version**
3. Select **Query All** and click **View**.
4. Verify the firmware release for each IPSI.
5. To upgrade a firmware:
   - Log in to the Avaya Support website at http://support.avaya.com.

- Click **Downloads**.
- In the pop-up window, type `Communication Manager`.
- In the list of downloads, click the link associated with the required firmware name.
- Click **Downloads**.
- Click the required firmware link.

Enabling control of the IPSIs

Procedure

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 30.
3. On the SAT screen, type **`change system-parameters ipserver-interface`** and press `Enter`.
4. Ensure that the **IPSI Control of Port Networks** field is set to enabled.
5. Press `Enter` to save the changes.

Chapter 6: Server roles

Communication Manager templates and their roles

You can configure a server on which a Communication Manager template is installed to one of the following permitted roles:

Communication Manager template	Permitted server role
Duplex Main/Survivable Core (Avaya Aura® CM Duplex)	MAIN or Survivable Core Server
Simplex Main/Survivable Core (Avaya Aura® CM Simplex)	MAIN or Survivable Core Server
Simplex Survivable Remote (Avaya Aura® CM_SurvRemote)	Survivable Remote Server
Embedded Survivable Remote (Avaya Aura® CM_onlyEmbed)	MAIN on Embedded Server
Embedded Survivable Core (Avaya Aura® CM_SurvRemoteEmbed)	Survivable Remote Server on Embedded Server

Verifying that the main server identifies the new survivable remote server

Before you begin

Configure a role for a main server, you must configure the survivable remote server. For more information on configuring a server role, see *Deploying Avaya Aura® Communication Manager on System Platform, 03-603558*.

Procedure

1. Wait for several minutes after you reset the survivable remote server.
2. On the main server, enter **`list survivable-processor`** to verify that the system registered the survivable remote server and updated the translations.

3. If the survivable remote server is registered, the **Service State** field shows `in-service` and the Translations Updated field shows the time and the date of the update.

```
list survivable-processor                                    Page   1 of  x
                          SURVIVABLE PROCESSORS
Record Name/            Type        Reg Act          Transactions      Net
Number  IP Address                                    Updated           Rgn
1      ESSCid020Sid097   ESS  S       n                                  1
        172.21.22.39
       No V6 Entry
2      ESSCid030Sid096   ESS  S       n                                  1
        172.21.22.40
       No V6 Entry
3      ESSCid040Sid095   ESS  S       n                                  1
        172.21.22.41
       No V6 Entry
4      ess1pe           ESS  D       n                                 26
        172.21.22.36
       No V6 Entry
```

Readminister branch gateways

If you include a survivable remote as an alternate controller, you must change the controller list for each Branch Gateway. With this change, the branch gateway can seek service from the survivable remote server if the connection to the main server fails.

Note:

Do not perform this task if you installed a new gateway and Communication Manager servers as part of the first time installation.

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

- *Installing and Upgrading the Avaya G430 Branch Gateway*, 03-603233
- *Installing and Upgrading the Avaya G450 Branch Gateway*, 03-602054

Chapter 7: Postinstallation administration

Verifying translations

Procedure

1. On the media server, open a SAT session.
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

Before you begin

Use the System Platform Web Console to set the date, time, and time zone on the server. You must use SAT commands to set the rules for daylight savings time.

Procedure

1. On the SAT screen, type **change daylight-savings-rules** and press **Enter**.

```
change daylight-savings-rules                                  Page   1 of   2
                        DAYLIGHT SAVING RULES
 Rule          Change Day                 Month  Date   Time    Increment
  0: No Daylight Saving
  1: Start: first            on or after March     8   at   :00     :
      Stop: first Sunday     on or after November  1   at 02:00
  2: Start: first            on or after               at   :       :
```

```
     Stop: first            on or after              at   :
  3: Start: first           on or after              at   :       :
     Stop: first            on or after              at   :
  4: Start: first           on or after              at   :       :
     Stop: first            on or after              at   :
  5: Start: first           on or after              at   :       :
     Stop: first            on or after              at   :
  6: Start: first           on or after              at   :       :
     Stop: first            on or after              at   :
  7: Start: first           on or after              at   :       :
     Stop: first            on or after              at   :
```

2. In the **Change Day**, **Month**, **Date**, **Time**, and **Increment** 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 gateways in several different time zones, you can set up rules for these 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 the default rule of 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 as necessary

Before you begin

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

Procedure

1. On the SAT screen, type **`change locations`** and press `Enter`.

```
change locations                                          Page   1 of   5
                                LOCATIONS
                ARS Prefix 1 Required For 10-Digit NANP Calls? y
Loc Name          Timezone DST    City/                          Proxy Sel
 No                Offset         Area                            Rte Pat
 1: Main            + 00:00  0
 2: CA              - 02:00  0
```

2. In the **ARS Prefix 1 Required for 10-Digit NANP Calls** field, type `y`.
   The system displays the location information.
3. Click **Submit** to save the changes.

Note:

The location of a port network is defined on the Cabinet screen using the **change cabinet X** command. The location of a network region is defined on the ip-network-region screen using the **change ip-network-region X** command. The location of a branch gateway is defined on the change media-gateway screen using the **change media-gateway X** command. The **Location** field in the ip-network-region SAT screen is part of the association to the daylight-savings-rule that an IP phone follows.

Verifying the date and the time of the main server

Procedure

1. On the SAT screen, type **display time** and press **Enter**.

```
display time                                                Page   1 of   1
                              DATE AND TIME
        DATE
            Day of the Week: Thursday        Month: June
           Day of the Month: 16               Year: 2011
        TIME
            Hour: 15 Minute: 6   Second: 45    Type: Standard
                        Daylight Savings Rule: 0
  WARNING: Changing the date or time may impact BCMS, CDR, SCHEDULED
EVENTS,
           and MEASUREMENTS
```

2. Verify that the date and the time of day are correct.
   If the date and the time of day are correct, go to step 5 on page 40.
   If the date and time of day are not correct, go to step 3.
3. Verify connectivity to any administered Network Time Server:
   a. On the System Platform Web Console, click **Server Management** > **Date / Time Configuration**.
   b. In the **Time Server** field, type the IP address of the Network Time Server.
   c. Click **Ping**. If the Network Time Server is not administered:
      i. On the left navigation menu, click **Server Date/Time**.
      ii. Set the correct date and time. Verify that the time zone is correct.

Note:

This operation reboots the server and disrupts the Communication Manager service.

Important:

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

4. Repeat steps 1 through 3.
5. Verify that the **Daylight Savings Rule** field is correct.
   - 0 indicates that this server is in a location that does not use daylight savings time.
   - 1-15 indicate the use of an administered rule using the SAT command **daylight-savings-rules**. For more information on the **daylight-savings-rules**, see Setting rules for daylight savings time on page 37.

     Note:

     The daylight savings rule setting on the Daylight Saving Rules screen is the rule that the Communication Manager software uses. You can implement additional daylight savings rules for the specific locations of hardware that the Communication Manager software supports. For more information, see Setting locations as necessary on page 38.

Clearing and resolving alarms

Procedure

1. Log in to System Management Interface.
2. Click **Administration** > **Server (Maintenance)** > **Current Alarms**.
   For duplicated servers, you can resolve alarms on the active server only.
3. Select the server alarms to clear and click **Clear Specific**.

   Note:

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

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all virtual machines) using System Platform Web Console.

Procedure

1. On the System Platform Web Console, click **Server Management** > **Data Backup/ Restore**.
2. Click **Backup Now**.

   Important:

   The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.
3. Select where to store or send the backup files:
   - SCP: Stores the backup archive files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol.
   - SFTP: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - FTP: Sends the backup archive file to an FTP server.
4. Enter other information as appropriate.
5. Click **Start Backup**.

Registering the system

Procedure

See the *Registering the system* of *Deploying section in Avaya Aura® Communication Manager on System Platform*, 18-604394.

Chapter 8: Installation verification

Testing the IPSI circuit pack

About this task

To test the clock and packet interface components within the circuit pack.

Procedure

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

Testing the license file

Before you begin

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

Procedure

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

Before leaving the site

Procedure

Provide the default LAN security settings to the customer.

LEDs

LEDs on the front panel of S8800 Server

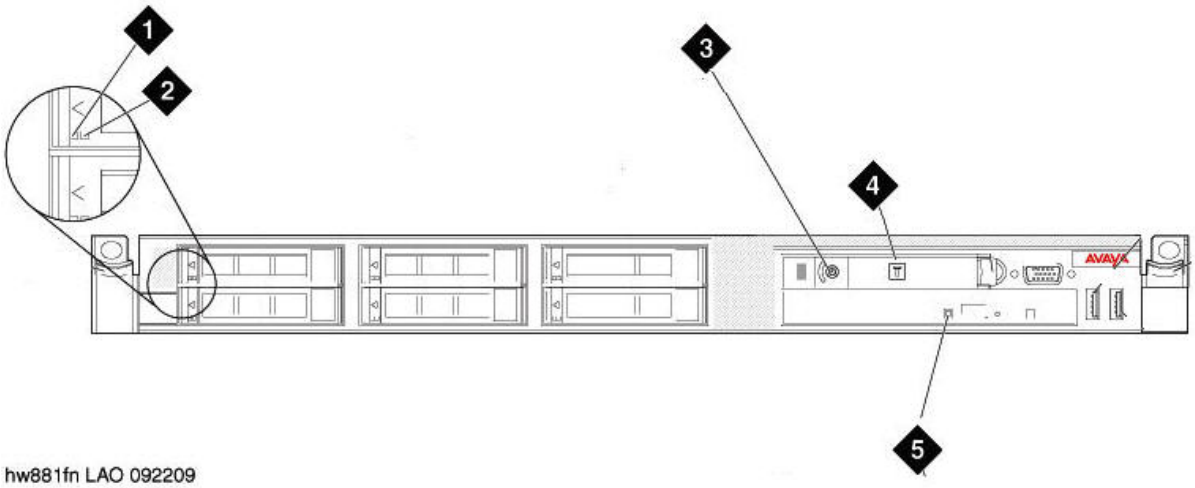

Figure 5: LEDs on the front panel of S8800 Server

Number	Description
1	Hard disk drive activity LED (green)
2	Hard disk drive status LED (amber)
3	Power on LED
4	Service Locator LED The LED indicates the following states: • Off: When the server is a simplex server or an active server in a duplex pair. No gateways are registered to the server, and the server is not the master of any port networks. • Flashing: When the server is the standby server of the pair. • Steady: When the server is the active server in a duplex pair. One or more gateways are registered to the server or the server is the master of one or more port networks. Alternatively, both gateways

Number	Description
	might be registered and the server acts as the master of port networks.
5	DVD drive activity LED

LEDs on the back panel of S8800 Server

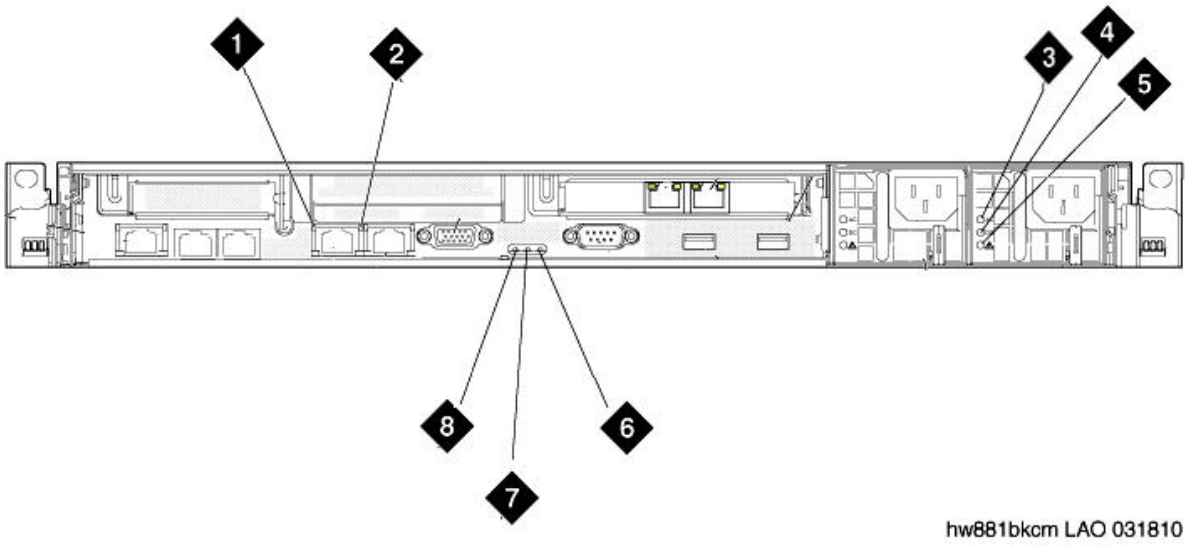

Figure 6: LEDs on the back panel of S8800 Server

Number	Description
1	Ethernet activity LED
2	Ethernet link LED
3	AC power LED (green)
4	DC power LED (green)
5	Power supply error LED (amber)
6	System error LED (amber)
7	System locator LED (blue)
8	Power LED (green)

LEDs on the front panel of Dell™ PowerEdge™ R610 1U Server

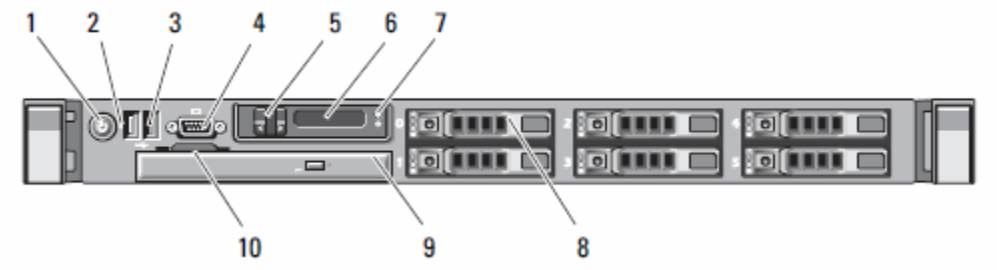

Figure 7: LEDs on the front panel of Dell R610 Server

Number	Description
1	Power-on indicator, power button
2	NMI button
3	USB connectors (2)
4	Video connector
5	LCD menu buttons
6	LCD Panel
7	System identification button
8	Hard drives
9	Optical drive
10	System identification panel

Dell R610 Server LEDs

The scrolling LCD and the back panel service LED reflects the active or standby status of the application:

Table 2: Dell R610 Server LEDs

Active/standby state	LCD behavior
Active	Blue backlight lights steadily to indicate the absence of errors. Amber backlight lights steadily to indicate the presence of errors.
Standby	Alternates between blue backlight and off in the absence of errors. Alternates between blue backlight, amber backlight, and off in the presence of errors.

Active/standby state	LCD behavior
Simplex	Blue backlight lit steady if no errors; amber backlight lit steady if errors

When you do not specify the active or standby state, the LCD follows the simplex behavior. The system ignores the application status and alarm requests.

LEDs on the back panel of Dell R610 Server

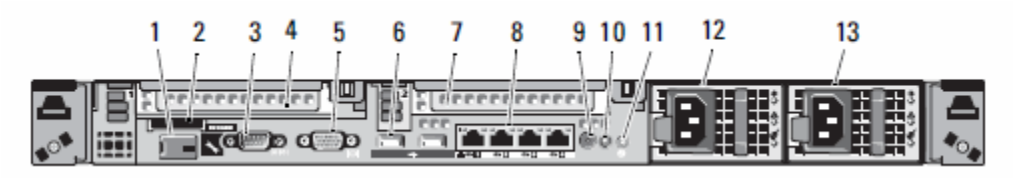

Figure 8: LEDs on the back panel of Dell R610 Server

Number	Description
1	iDRAC6 Enterprise/Express port (optional)
2	VFlash media slot (optional)
3	Serial connector
4	PCIe slot 1
5	Video connector
6	USB connectors (2)
7	PCIe slot 2
8	Ethernet connectors (4)
9	System status indicator connector
10	System status indicator
11	System identification button
12	Power supply 1 (PS1)
13	Poser supply 2 (PS2)

LEDs on the front panel of HP ProLiant DL360 G7 1U Server

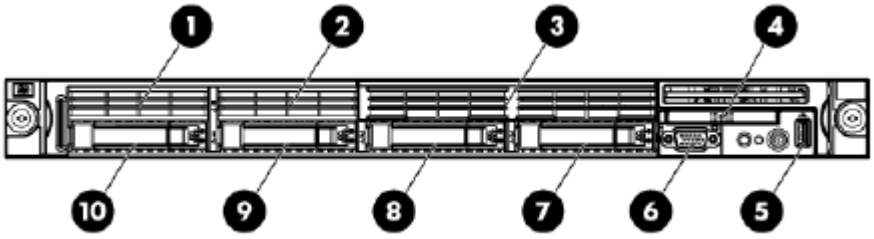

Figure 9: LEDs on the front panel of HP DL360 G7 Server

Number	Description
1	Hard disk drive not present.
2	Hard disk drive not present.
3	Activity LED on DVD-RW drive intermittent when DVD is loaded.
4	Systems Insight Display has several LEDs to indicate problems with: • Processor • DIMMs • Fans • Temperature • Power supply • Power capacity
5	Front USB connector
6	Video connector
7	Hard disk drive LEDs
8	Hard disk drive LEDs
9	Hard disk drive LEDs
10	Hard disk drive LEDs

LEDs on the back panel of HP DL360 G7 Server

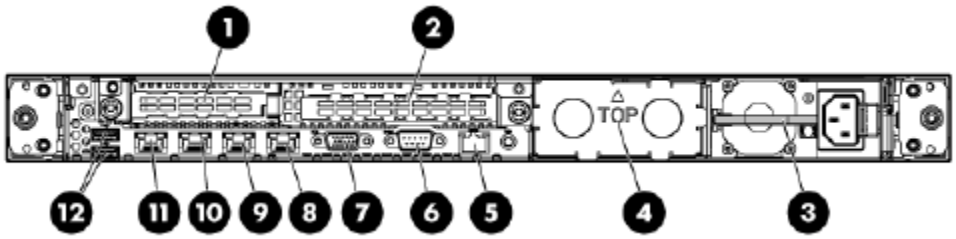

Figure 10: LEDs on the back panel of HP DL360 G7 Server

Number	Description
1	Slot 1 PCIe2 x8 (8, 4, 2, 1) **Note:** You require a half HT faceplate. You might need to remove the full faceplate and replace the faceplate with a half faceplate using a Phillips screwdriver. To add a NIC, use PCI Slot 1 prior to slot 2. This sequence applies to NICs only.
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1), 75W +EXT 75W*
3	Power supply LEDs
4	Optional power supply LEDs
5	iLO 3 connector
6	Serial connector
7	Video connector
8	NIC LEDs
9	NIC LEDs
10	NIC LEDs
11	NIC LEDs
12	USB connectors (2)

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.

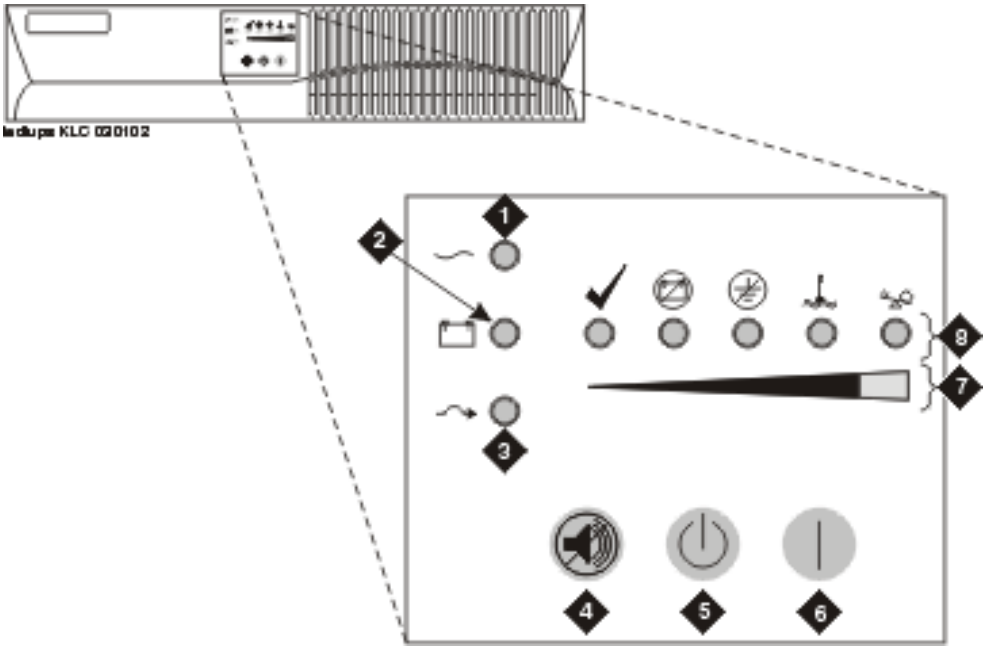

Figure 11: LEDs on the Powerware 9125 UPS

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

TN2312BP IPSI LEDs

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

- Standard LEDs and connector slots. See *TN2312BP IPSI circuit pack faceplate*.
- A programmable LED display, which indicates a static address, the display shows `I P`. See *IPSI LED display for IP address*.

For more information on troubleshooting the configuration of the server hardware, see *Installation troubleshooting*.

TN2312BP IPSI circuit pack faceplate

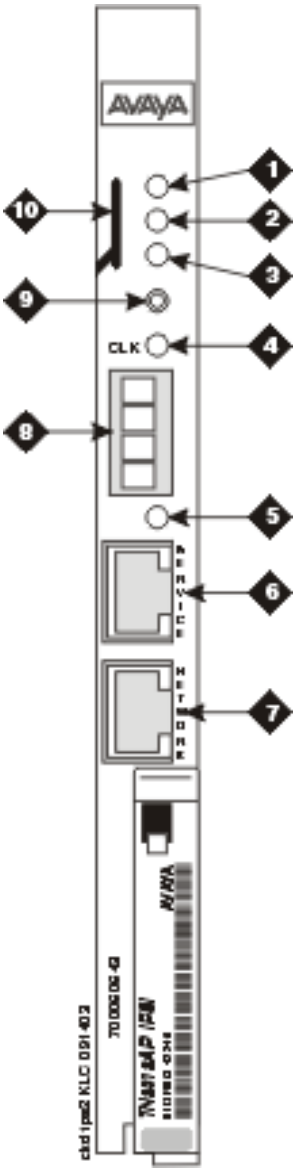

Figure 12: TN2312BP IPSI circuit pack faceplate

Number	Description
1	Red LED
2	Green LED
3	Amber LED
4	Yellow LED (tone clock status)

Number	Description
5	Emergency transfer LED
6	Services RJ45 connector
7	Network control RJ45 connector
8	Four-character LED display
9	Pushbutton switch
10	Slot for the maintenance cable

IPSI LED display for IP address

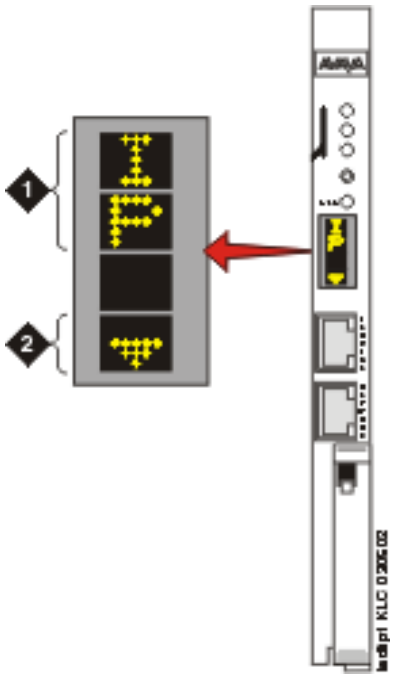

Figure 13: IPSI LED display for IP address

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

Appendix A: Installation troubleshooting

Troubleshooting the installation of the server hardware

No power to the UPS

Powering of the UPS

Procedure

1. Ensure that the UPS is plugged into the outlet.
2. Ensure that the outlet has power.
3. For other solutions, see the user guide for the UPS.

No power to the server

Powering UPS

Procedure

1. Ensure that the circuit pack is seated.
2. Ensure that the media gateway is plugged into the UPS.
3. Ensure that the UPS has power.
4. Push the power button on the front of the server.

Note:

"No power to the server" means that the server is not functioning, probably because it is not receiving power supply.

The IPSI LEDs flash

Flashing of IPSI LEDs

Procedure

1. Ensure that the IPSI is in the correct slot. Use slot 1 for the G650 Media Gateway.
2. Ping the IPSI from server.
3. Ping the server from the IPSI.

Troubleshooting the configuration of the server hardware

Cannot log in to the UPS subagent

Logging into UPS subagent

Procedure

1. Ensure that the SNMP subagent is installed in the UPS.
2. Ensure that you are connected to the correct Ethernet port.
3. Ensure that you have the correct log-in ID and password. For more information, see the user guide for the SNMP subagent.
4. Ensure that the network card on the laptop computer is configured correctly.

Cannot log in to the server

Logging into the server

Procedure

1. Check the link LED on the server. If the LED is off, a cable or hardware problem exists.
2. Ensure that you are using SSH and not telnet.
3. Ensure that you are connected to the Services Ethernet port.
4. Ensure that you are using a cross-over cable between the Services laptop computer and the server.
5. Ensure that the ARP cache is cleared on the Services laptop computer. In an MS-DOS window, type **arp** -d <Avaya Aura CM virtual machine IP address> and press `Enter`.
6. Ensure that you have connectivity. In an MS-DOS window, type **ping** <Avaya Aura CM virtual machine IP address> and press `Enter`.
7. Ensure that the NIC on the Services laptop computer is configured correctly.

Cannot access the SAT

Accessing the SAT screen

Procedure

1. Ensure that you are using the correct IP address and port 5022.
2. Ensure that you are using SSH and not telnet.
3. Ensure that you are using the correct login and password.

Cannot ping out to the customer network

Pinging out to the customer network

Procedure

Ensure that in the LAN security settings *output from server* for icmp is enabled.

Cannot ping the server from the customer network

Pinging the server from customer network

Procedure

Ensure that in the LAN security settings *input to server* for icmp is enabled.

Cannot access the server remotely

Accessing the server remotely

Procedure

Ensure that in the LAN security settings *input to server* is checked for SSH (Linux commands), https (Web access), and def-sat (SAT commands access). Change the LAN security settings on the Web interface with a direct connection to the server.

The LED display flashes on IPSI

An IP address is not assigned to the IPSI LED static IP addressing.

Cannot access the IPSI

Accessing the IPSI

Procedure

1. Ensure that you are plugged into the Services (top) port on the .
2. Ensure that the ARP cache is cleared on the Services laptop computer. In an MS-DOS command window, type **`arp -d 192.11.13.6`** and press `Enter`.

No *V* shows on the IPSI LED

The IPSI is not connected to the network.

Displaying the IPSI LED

Procedure

Connect a cable to the bottom port on the faceplate and to the customer network.

The *V* on the IPSI LED is not filled in

- An IPSI address is not assigned to the IPSI.
- The IPSI is not administered.

The system generates an alarm when first connect to IPSI

The IPSI does not have the current firmware.

Alarming on connection to IPSI

Procedure

Upgrade the firmware.

Unable to log in to the server

Logging in to the server

Procedure

If you are connecting the laptop to the services port of the server, ensure that IP forwarding is enabled at the System Domain (Domain-0) command line.

Problem	Possible solution
Cannot access the Avaya Installation Wizard	• Ensure that you are plugged into the Services port. • Ensure that you are using SSH and not telnet. • Ensure that you are using the correct IP address, 192.11.13.6 • Ensure that you are using the correct login and password. • Ensure that the NIC on the laptop is configured correctly.

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

Cannot get license file from the PLDS site

Licensing from the PLDS site

Procedure

1. Provide the correct LAC.
2. Search for your entitlements and locate the LAC. See “Searching for entitlements” in Getting Started with Avaya PLDS.

Cannot install the license file on the WebLM server

Installing the license file on the WebLM server

Procedure

The file might be corrupt. Download the file again from PLDS.

Note:

If the license file cannot be installed on the WebLM server, the WebLM server returns an error message, indicating why the file will not install. Read the WebLM error message and correct the problem as indicated in the error message. A corrupt file is one of the reasons why the file might not install.

The server is in no-license mode

Licensing mode

Procedure

Download a license file from PLDS and install it on the WebLM server.

Note:

If Communication Manager is in no-license mode, the system indicates the nature of the error. Read the error message and correct the problem as indicated in the error message. A missing file is one of the reasons why Communication Manager is in no-license mode.

Cannot use the administration commands

The server might be in no license mode because the 30-day grace period has expired.

Using administration commands

Procedure

Download a license file from PLDS and install the file in WebLM.

Result

See the troubleshooting step for the server being in no-license mode.

ASG on Avaya services logins does not work

Using ASG logins

Procedure

1. Reinstall the Avaya authentication file on the System Platform Console Domain.
2. If ASG on Avaya services logins still does not work, create a replacement authentication and install the authentication file on the System Platform Console Domain.

Authentication file installed on the System Platform Console Domain is not present on the Communication Manager server

Missing file on the Communication Manager server

Procedure

Administer a super-user login on the active server.

Index

S

T

U

V

W