Upgrading to Avaya Aura® Communication Manager

Release 6.0.1
03-603560
Issue 3.0
January 2011

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.

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 Web sites 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.

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 Web site: 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.

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 End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, 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.
- Named User License (NU). End User 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). Customer 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"). (see "Third-party Components" for more information).

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.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those

Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura® are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) 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(s) 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.

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

Downloading Documentation

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

Contact 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://support.avaya.com.

Contents

Chapter 1: Introduction

Communication Manager upgrades

This book provides the process and procedures for upgrading Avaya Aura® Communication Manager to Release 6.0.1. Communication Manager is an application that resides on a virtual server. The underlying framework is called Avaya Aura® System Platform. Communication Manager is a template that runs on System Platform.

Communication Manager was known as Avaya Aura® MultiVantage in Release 1.1 and Release 1.2.

This book provides the following upgrade procedures:

- Software-only upgrade: Upgrading Communication Manager from Release 6.0 to Release 6.0.1.
- Hardware and software upgrade: Replacing the existing server with the server that Communication Manager Release 6.0.1 supports.
    - For systems on Release 5.2.1, upgrading from Release 5.2.1 to Release 6.0.1.
    - For systems on Release 4.0.5, upgrading from Release 4.0.5 to Release 6.0.1.
    - For systems between Release 5.0 and Release 5.2:
        i. Upgrading from the existing release to Release 5.2.1.
        ii. Upgrading from Communication Manager Release 5.2.1 to Release 6.0.1.
    - For systems on a release earlier than 4.0.5:
        i. Upgrading from the existing release to Release 4.0.5.
        ii. Upgrading from Communication Manager Release 4.0.5 to Release 6.0.1.

Beginning with Release 6.0.1, Communication Manager runs on the following servers:

- Avaya S8300D Server
- Avaya S8510 Server
- Avaya S8800 Server

- Dell™ PowerEdge™ R610 Server
- HP ProLiant DL360 G7 Server

You can upgrade Communication Manager from Releases 5.2.1 or Release 6.0 to Release 6.0.1 on the following servers:

- S8300D Server
- S8510 Server
- S8800 Server
- HP ProLiant DL360 G7 Server

Note the following upgrade considerations:

- Any servers that are on Communication Manager Release 5.2.1 or Release 6.0 are upgraded to Release 6.0.1 on the existing servers.
- Any servers that are on Communication Manager Release 5.0 or release earlier than 5.2.1 must be upgraded to Release 5.2.1 before you upgrade them to Release 6.0.1 unless otherwise noted
- Any servers that are on a release earlier than 4.0.5 must be upgraded to Release 4.0.5 before you upgrade them to Release 6.0.1 unless otherwise noted.

System Platform

Avaya Aura® System Platform technology delivers simplified deployment of Unified Communications and Contact Center applications. This framework leverages virtualization technology, predefined templates, common installation, licensing, and support infrastructure.

The advantages of System Platform include:

- Ability to install predefined templates of one or more Avaya software applications on a single server in a virtualized environment
- Simplified and faster installation of software applications and solutions
- Remote access and alarming for Avaya Services and Avaya Partners

System Platform enables real-time communications solutions to perform effectively in a virtualized environment. System Platform effectively manages the allocation and sharing of server hardware resources, including the CPU, memory, disk storage, and network interfaces. To continue delivering the high reliability of real-time communications that Avaya customers expect, System Platform is being delivered solely through an *appliance* model, which includes an Avaya Server, System Platform, and the Avaya software applications.

Communication Manager templates overview

Communication Manager as a template is a virtualized version that runs on System Platform. This image has all the features that Communication Manager supports whether it is on a duplicated server or a branch server. The templates support Communication Manager duplication on S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. The templates support Communication Manager which configures as Main, Survivable Core (formerly known as Enterprise Survivable Server - ESS), or Survivable Remote (formerly known as Local Survivable Processor - LSP). In addition, the templates allow customers to use their network infrastructure without dedicated control networks.

Note:

The Communication Manager installation and administration Web pages refer to Survivable Core as Enterprise Survivable Server (ESS) and Survivable Remote as Local Survivable Processor (LSP), respectively.

The advantages of using a solution as a template on System Platform are as follows:

- Simplified and faster installation of the solution
- Simplified licensing of applications and solutions
- Web Console with a common Avaya look and feel
- Remote access and alarming for Avaya Services and Avaya Partners
- Coordinated backup and restore
- Coordinated software upgrades

The Communication Manager templates come in two categories: Avaya Aura® for Communication Manager Main/Survivable Core and Avaya Aura® for Communication Manager Survivable Remote. The templates in each category are listed below:

- Avaya Aura® for Communication Manager Main/Survivable Core template category contains the following templates:
    - Simplex CM Main/Survivable Core
    - Duplex CM Main/Survivable Core
    - Embedded CM Main
- Avaya Aura® for Communication Manager Survivable Remote template category contains the following templates:
    - Simplex Survivable Remote
    - Embedded Survivable Remote

Avaya Aura® for Communication Manager Main/Survivable Core

The Communication Manager Main/Survivable Core templates include the following applications:

- Communication Manager
- Communication Manager Messaging

  Note:

  Communication Manager Messaging is available only if Communication Manager is configured as the main server. Communication Manager Messaging and Utility Services are not available on Duplex Main/Survivable Core.

- Utility Services

Both Simplex Main/Survivable Core and Duplex Main/Survivable Core templates can be installed on an S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. The Simplex Main/Survivable Core can be installed on an S8510 Server with a total 8 Gb memory as an upgrade only. The Embedded Main template is installed on an S8300D Server in either a G250, G350, G430, G450, or G700 Branch Gateway.

Avaya Aura® for Communication Manager Survivable Remote

The Communication Manager Survivable Remote templates include the following applications:

- Communication Manager
- Branch Session Manager
- Utility Services

The Simplex Survivable Remote is installed on an S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. Simplex Survivable Remote can be installed on an S8510 Server with 8 Gb memory as an upgrade only. Embedded Survivable Remote is installed on S8300D Server in either a G250, G350, G430, G450, or G700 Branch Gateway. Both templates are used in the following two scenarios:

- Communication Manager Evolution Server
- Communication Manager Feature Server

Note:

For information on template capacities, refer to the *Avaya Aura® Communication Manager System Capacities Table*.

Communication Manager Release 6.0.1 survivable servers

The table defines the platforms that can be a survivable remote server or survivable core server.

Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.

Primary server	Survivable servers			
	System Platform S8300	System Platform S8510	System Platform (S8800)	
			Simplex	Duplex
Simplex System Platform (S8300D)	Survivable remote	Not applicable	Not applicable	Not applicable
Simplex System Platform (S8510)	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Simplex System Platform (S8800)	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Duplex System Platform (S8800)	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core

Obtaining and installing the license file

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later. PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

Earlier versions of Communication Manager, except Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template, continue to use the Remote Feature Activation (RFA) online tool for license files. Communication Manager 5.2.1 that is part of Avaya Aura®Midsize Business Template uses PLDS to manage licenses. After you obtain the license file, use WebLM to install it. WebLM is a Web-based application for managing licenses and is installed as part of System Platform in the Console Domain.

The license file is an Extensible Markup Language (XML) file. It contains information regarding the product, major release, and license features and capacities.

For Communication Manager 6.0 and later, license files are installed only on the Communication Manager main server. License files are not installed on survivable servers. Survivable servers receive licensing information from the main server.

If you are licensing a duplicated pair configuration, you must install the license file on both servers. The license file is not synchronized from the active server to the standby server.

A 30-day grace period applies to new installations or upgrades to Communication Manager 6.0. You have 30 days from the day of installation to install a license file.

Duplicated server licensing

If you are licensing a duplicated pair configuration, you must install the license file on both servers. The license file is not synchronized from the active server to the standby server.

When you activate a Communication Manager license file for a duplicated pair in PLDS, you must provide the WebLM host ID for both servers. Both host IDs are included in the license file that is generated, and that license file must be installed on both servers in the duplicated pair.

Authentication files for Communication Manager

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for Communication Manager. ASG keys make it possible for Avaya Services to securely access the customer's system.

System Platform and Communication Manager share the same authentication file. A default authentication file is installed with System Platform. However the default file must be replaced with a unique file. Unique authentication files are created by the Authentication File System (AFS), an online application at http://rfa.avaya.com. After you create and download the authentication file, you install it from the System Platform Web Console of the Communication Manager server. When you install the authentication file in System Platform, the file is automatically installed on Communication Manager, Utility Server, and any other virtual machines on the server.

Every time that you upgrade Communication Manager to a new major release, you need to create and install a new authentication file.

Authentication files for duplicated servers and survivable servers

For duplicated pair configurations, you must install the same authentication file on both the active server and standby server. The authentication file is not synchronized from the active server to the standby server.

Each survivable server must have its own unique authentication file. A unique file must be installed from the System Platform Web Console of each server.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies it. You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

Use of third-party certificates

Many companies use third-party certificates for security. These certificates are not retained as part of the upgrade dataset and must be reinstalled after the upgrade. If you use third-party certificates, make sure you have a copy of them or download new ones before starting the upgrade.

Upgrade paths

The following table provides the upgrade paths to Release 6.0.x. Notice that some servers cannot be upgraded to Release 4.0.5 or Release 5.2.1 directly and require an upgrade to a new server on Release 4.0.5 or Release 5.2.1, respectively, before completing the upgrade to Release 6.0.x.

Release	Requirement
Release 1.x.x (DEFINITY R)	Requires restoring translations to an S8800 Server on Release 6.0.x.
Release 2.x (DEFINITY SI)	Requires restoring translations to an S8300D or S8800 Server on Release 6.0.x.
Release 3.x.x (DEFINITY CSI)	Requires restoring translations to an S8300D or S8800 Server on Release 6.0.x.
Release 1.x.x (S8300A)	Requires upgrading to an S8300D Server on Release 4.0.5 first before upgrading to Release 6.0.x.
Release 1.x.x (S8700)	Requires upgrading to an S8800 Server on Release 4.0.5 first before upgrading to Release 6.0.x.
Release 2.x.x (S8300A)	Requires upgrading to an S8300D Server on Release 4.0.5 first before upgrading to Release 6.0.x.
Release 2.x.x (S8500A, S8700, S8710 wDAL1)	Requires upgrading to an S8800 Server on Release 4.0.5 first before upgrading to Release 6.0.x.
Release 2.x.x (all other servers)	Requires upgrading to Release 4.0.5 first and installing a preupgrade service pack before upgrading to Release 6.0.x.

Release	Requirement
Release 3.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Requires upgrading to an S8800 Server on Release 4.0.5 first before upgrading to Release 6.0.x.
Release 3.x.x (all other servers)	Requires upgrading to Release 4.0.5 first and installing a preupgrade service pack before upgrading to Release 6.0.x.
Release 4.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Requires upgrading to an S8800 Server on Release 5.2.1 first before upgrading to Release 6.0.x.
Release 4.x.x (all other servers)	Requires upgrading to Release 5.2.1 first and installing a pre-upgrade service pack before upgrading to Release 6.0.x.
Release 5.0.x	Requires upgrading to Release 5.2.1 first and installing a pre-upgrade service pack before upgrading to Release 6.0.x.
Release 5.1.x	Requires upgrading to Release 5.2.1 first and installing a pre-upgrade service pack before upgrading to Release 6.0.x.
Release 5.2.1	Requires installing a preupgrade service pack before upgrading to Release 6.0.x.
Release 6.0	Requires software-only upgrades to Release 6.0.x.

Support for SIP Enablement Services

SIP Enablement Services in any form factor is not compatible with Communication Manager Release 6.x or later. If you are upgrading to Communication Manager Release 6.x, and you have SIP Enablement Services Release 5.2.1 or earlier deployed on the system, you need to install Avaya Aura® Session Manager for continued support of SIP stations and adjuncts. Contact your salesperson about the Avaya Aura®Session Manager option.

Special circumstances

Consider the following special situations when upgrading Communication Manager to Release 6.x.

- If you have Communication Manager Messaging or Intuity Audix 770 enabled on the existing system, backup and restore that dataset separately on the upgraded system.
- If you have Communication Manager and SIP Enablement Services (SES) coresident on the S8300 server, you cannot restore SES on the new server. Because Communication Manager Release 6.x does not support SES.
- If you use Unicode phone messages on the existing system, reinstall the Unicode phone messages file after the upgrade.

Preupgrade requirements

For a successful upgrade, it is important that you are prepared well in advance. Some tasks are best done days before the upgrade. Make sure that you have:

- All of the hardware ordered and on site
- All of the software and service packs downloaded and easily available
- The needed applications on the computer you use to perform the upgrade
- A server identified with adequate disk space to store the datasets
- *For DEFINITY Server upgrades only*: Updated translations from the STS team

Hardware requirements

You need the following hardware to complete upgrade process:

Note:

Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.

- S8800 Server, if replacing an existing standalone server that cannot be upgraded to Release 6.0 or later.
- S8300D Server, if replacing an existing embedded server that cannot be upgraded to Release 6.0 or later.
- Release 6.0 Migration Kit for S8510 Server or S8800 Server if reusing the existing servers
- Required Ethernet CAT5 cables
- About five blank DVDs on which you burn the iso images.

Software requirements

You need to download the following software from appropriate Web site:

- System Platform from PLDS
- The Communication Manager templates from PLDS

- The license file from PLDS. You must have the MAC address from the System Platform Console Domain, as displayed on the Server Properties page of the WebLM server.
- The authentication (password) file from the Authentication File System (AFS).
- Preupgrade and postupgrade service packs from Avaya Support Web site (http://support.avaya.com).

Application requirements

You need the following applications installed on your computer:

- Internet Explorer 7.x browser
- Firefox 2.x or 3.x browser (supported by System Platform only)
- a Secure Shell application such as PuTTY.

Upgrade order

Upgrade in the following order if Communication Manager is part of Avaya Aura® core.

1. Endpoints
2. Avaya Aura® System Manager
3. Avaya Aura® Session Manager
4. Survivable remote servers (Communication Manager and System Manager)
5. Branch gateways (formerly called media gateways)
6. Survivable core servers
7. Communication Manager (Feature Servers and Evolution Servers)

Upgrade process

The process described in this section applies to the upgrade paths that start with a server running Communication Manager Release 4.0.5 and Release 5.2.1.

The following list provides the high-level upgrade sequence. You must complete the upgrade in this order.

1. Latest firmware on all Avaya H.248 Branch Gateways
2. Latest firmware on the media modules within the H.248 Branch Gateways
3. Communication Manager on any survivable remote server (formerly local survivable processors)

4. Communication Manager on any survivable core server (formerly enterprise survivable servers)
5. Communication Manager on the main server
6. Latest firmware on all TN circuit packs (if using port networks)
7. Latest firmware on all telephones

You need to complete the following general tasks on a simplex server when replacing the server.

Task	Notes	√
Verify that you have the required server and other hardware available on the site.		
Verify that you have the required software and pre- and post-upgrade service packs on hand.		
Verify that you have server and disk space available to back up the upgrade data set. You cannot use a flashcard to restore files to System Platform.		
Verify that you have all of the documentation and release notes on hand.		
For DEFINITY Servers: • Save and freeze translations. • Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.		
Record the IP addresses and other data on the existing server that you need to install System Platform and Communication Manager.	Use the worksheets provided in the appendices to make sure that you capture all the needed information.	
Convert private control networks to the corporate LAN.	Release 6.0.x does not support private networks (CNA and CNB). For instructions, see Introduction on page 1371.	
Complete the routine preupgrade tasks on the existing server.		
Back up all the files on the existing server in case you need to roll back to the original release.		
Install the preupgrade service pack on the existing server.		

Task	Notes	√
Back up the Communication Manager data set to be restored on the new server.		
Back up the Communication Manager Messaging data set to be restored on the new server if messaging is enabled.		
If a standalone server, shut down the existing server and remove all power cords and cables. If an embedded server, remove all cables from the faceplate, shut down the existing server and remove it from the H.248 Branch Gateway.		
Install one of the following server in the rack and connect the power cord and cables: • HP ProLiant DL360 G7 Server • Dell™ PowerEdge™ R610 Server • S8800 Server • S8300D Server (install in a branch gateway)	You can install the new server before completing the tasks on the existing server. Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.	
Install System Platform on the server.	On the new server, you can do this before completing the tasks on the existing server.	
Get the license file from PLDS and install it on the WebLM server accessed through the System Platform Web Console.	On the new server, you can do this before completing the tasks on the existing server.	
Get the authentication file from AFS and install through the System Platform Web Console.	On the new server, you can do this before completing the tasks on the existing server.	
Install the appropriate Communication Manager template through the System Platform Web Console.	On the new server, you can do this before completing the tasks on the existing server.	
Install postupgrade service pack (if required) through the System Platform Web Console.		
Restore the Communication Manager dataset through the System Platform Web Console.		
Configure Communication Manager through System Management Interface.	System Management Interface (SMI) was formerly known as Maintenance Web interface.	

Task	Notes	√
Reboot the server through System Platform Web Console or System Management Interface. **Important:** Check the status of other devices and applications dependent on Communication Manager such as Call Management System (CMS) and Call Center. Reboot the applications if required, after you complete the Communication Manager upgrade.		
Restore the Communication Manager Messaging data set through the System Management Interface.		
Configure Communication Manager Messaging.		
Complete the post-upgrade administration.		
Back up all the files.		
Register the upgraded system.		

Required documents

You require the following documents to complete the upgrade process. All documents are available on Avaya Support under the Communication Manager product name.

Title	Release	Notes
Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603444	6.x.x	Covers installing the S8800 Server in a rack.
Installing the Dell™ PowerEdge™ R610 Server	6.x.x	Covers installing the Dell™ PowerEdge™ R610 Server in a rack.
Installing the HP ProLiant DL360 G7 Server	6.x.x	Covers installing the HP ProLiant DL360 G7 Server in a rack.
Quick Start for Hardware Installation: Avaya G250 Media Gateway, 03-300433	5.2.x	Covers installing the S8300D Server in the G250 Branch Gateway.

Title	Release	Notes
Quick Start for Hardware Installation: Avaya G350 Media Gateway, 03-300148	5.2.x	Covers installing the S8300D Server in the G350 Branch Gateway.
Quick Start for Hardware Installation: Avaya G430 Media Gateway, 03-603236	5.2.x	Covers installing the S8300D Server in the G430 Branch Gateway.
Quick Start for Hardware Installation: Avaya G450 Media Gateway, 03-602053	5.2.x	Covers installing the S8300D Server in the G450 Branch Gateway.
Quick Start for Hardware Installation: Avaya G700 Media Gateway, 555-233-150	5.2.x	Covers installing the S8300D Server in the G700 Branch Gateway.
Installing and Configuring Avaya Aura™ Communication Manager, 03-603558	6.x.x	Covers installing System Platform, Communication Manager, license file, and authentication file.
Installing and Upgrading the Avaya S8300 Server, 555-234-100	5.2.x	Covers upgrading Communication Manager to Release 5.2 on the S8300A/B/C/D Server.
Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers, 03-602885	5.2.x	Covers upgrading Communication Manager to Release 5.2 on the Avaya S8500–series and S8700–Series Servers.
Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603446	5.2.x	Covers upgrading the Avaya S8500–series and S8700–Series Servers to the S8800 Server.

How to use the books

This book is organized first by Communication Manager template and then by existing server. For example, if you are upgrading Communication Manager 5.2.1 on an S8500 Server to the main/survivable core simplex template on an S8800 Server, go to the “Upgrading to simplex main/survivable template” chapter and look for Upgrading S8500 Server to the S8800 Server section.

Additionally, you require to refer more books to successfully complete the upgrade. The following roadmap provides a list of high-level tasks and the book you need to use for that part of the upgrade.

Table 1: Task to book roadmap

Task	Book to use	Notes
Upgrade Communication Manager to Release 4.0.5 or Release 5.2.1 for servers that can be.	*Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers*, 03-602885	You can upgrade most Linux-based servers to Release 5.2.1.
Upgrade Communication Manager to Release 4.0.5 or Release 5.2.1 for servers that cannot be.	*Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager*, 03-603446	You must upgrade the Linux-based servers, which you cannot upgrade directly to Release 4.0.5 or Release 5.2.1 to the new server first. Those servers include: • S8300A • S8500A • S8700 • S8710 with DAL1 • S8720 with DAL1
Download files from PLDS and AFS	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Record required data	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	
Complete the routine preupgrade tasks on the existing server.	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	
Back up all the files on the existing server in case you need to roll back to the original release.	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	
Install the preupgrade service pack on the existing server.	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	
Back up all the data sets to be restored on the new server.	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	

Task	Book to use	Notes
Install the server in the rack	Use one of the following books as appropriate: • *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager*, 03-603444 • *Installing the Dell™ PowerEdge™ R610 Server* • *Installing the HP ProLiant DL360 G7 Server*	
Install the S8300 Server in the branch gateway.	*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 G430 Media Gateway*, 03-603236 *Quick Start for Hardware Installation: Avaya G450 Media Gateway*, 03-602053 *Quick Start for Hardware Installation: Avaya G700 Media Gateway*, 555-233-150	Refer to the book for your particular Gxxx branch gateway.
Install System Platform on the server.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Install license and authentication files	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Install the appropriate Communication Manager template through the System Platform Web Console.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Install postupgrade service pack (if required).	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	
Restore the datasets on the new server	*Upgrading to Avaya Aura™ Communication Manager*	

Task	Book to use	Notes
	Release 6.0, 03-603560 (this book)	
Configure Communication Manager through the System Management Interface.	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	It is important that you use this book to configure Communication Manager.
Complete the postupgrade administration.	*Upgrading to Avaya Aura™ Communication Manager Release 6.0*, 03-603560 (this book)	

Chapter 2: Upgrading from Release 6.0 to Release 6.0.1

Upgrading from Release 6.0 to 6.0.1 on simplex main/ survivable template

Introduction

This section describes the procedure to upgrade the Communication Manager software from Release 6.0 to Release 6.0.1 on the server running System Platform and the simplex main/ survivable core template (CM_Simplex).

You perform this software-only upgrade using one of the following methods:

- Onsite by connecting the laptop to the services port on the server.
- Remotely by accessing the server through the corporate network.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Backing up translations, security, and system files.
- Upgrading System Platform and the Communication Manager template.
- Performing the upgrade to Release 6.0.1 as described in this section.

The upgrade procedure preserves Communication Manager translations, administrator accounts, Communication Manager Messaging files, and the server configuration. You do not require the following files during the upgrade:

- A new or updated license file
- An authentication file

Use this section to upgrade Communication Manager from Release 6.0 to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the Communication Manager template (as appropriate)	
	Obtain one of the following servers, as appropriate: • S8800 Server • Dell™ PowerEdge™ R610 Server • HP ProLiant DL360 G7 Server	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the latest service packs and the required software. • System Platform • Communication Manager template	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the existing system

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled

for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   1. Start an SSH session.
   2. Log in to System Domain (Domain-0) as admin.
   3. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   1. Start an SSH session.
   2. Log in to System Domain (Domain-0) as admin.
   3. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.
   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

You back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Important:

If Communication Manager Messaging is enabled on your system, back up the messaging data using System Management Interface.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

Note:

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
    - If Communication Manager Messaging is not enabled:

      Select **Full Backup**.

      The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.
    - If Communication Manager Messaging is enabled:
        i. Select **Specify Data Sets**.
        ii. Select the following check boxes:
            - **Avaya Call Processing (ACP) Translations**
            - **Server and System Files**
            - **Security Files**
            - **Communication Manager Messaging (CMM)**

              Select **Translations, Names, and Messages**.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**. Enter the host IP address
    - **Directory**

When the backup process is complete, the system saves the `*.tar.gz` file to the `/var/home/ftp/pub` location.

6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   > ⚠ **Caution:**
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.
   If you find any announcement sets other than the following, proceed with Step 3:
   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. On the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Upgrade tasks

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Upgrading System Platform

Prerequisites

Log on to the System Platform Web console.

Perform the upgrade of System Platform and install the latest service packs or patches.

- System Platform
- System Platform service pack as instructed in Installing patches on page 45.
- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 45.

1. Under **Server Management**, click **Platform Upgrade**.
2. Select the method you adopt for upgrade.
3. Select the file to install for System Platform and click **Select**.
4. Click **Install**.

Next steps

Install the service pack and patches for System Platform as instructed in Installing patches on page 45.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Upgrading the Communication Manager template

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Solution Template**.
2. Select the method you use to access the template.
3. Select the Communication Manager template.
4. Click **Upgrade**.
   The system automatically does the following:
   - Backs up Communication Manager.
   - Installs the new Communication Manager.
   - Restores Communication Manager from the backed up data.

Next steps

Install the service pack and patches for Communication Manager as instructed in Installing patches on page 45.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.

2. Verify the following:

   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system

Prerequisites

Start a SAT session.

Enter `list station` and verify that the stations listed after the upgrade are the same as the stations listed before the upgrade.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

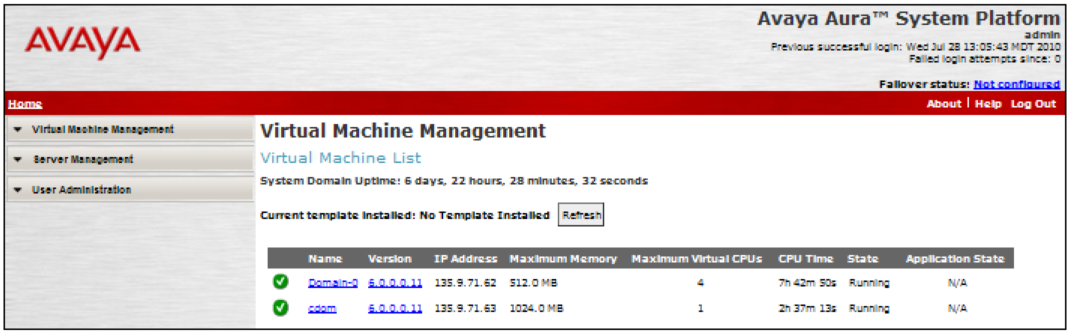
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:

   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading from Release 6.0 to 6.0.1 on duplex main/survivable template

Introduction

This section describes the procedure to upgrade Communication Manager software from Release 6.0 to Release 6.0.1 on the servers running System Platform and the duplex main/survivable core template (CM_Duplex).

The upgrade procedure involves:

- Backing up translations, security, and system files.
- Upgrading System Platform and Communication Manager template.
- Performing the upgrade to Release 6.0.1 as described in this section.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and the server configuration. You do not require the following files during the upgrade:

- A new or updated license file
- An authentication file

Use this section to upgrade Communication Manager from Release 6.0 to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the Communication Manager template (as appropriate)	
	Obtain one of the following servers, as appropriate: • S8800 Server • Dell™ PowerEdge™ R610 Server • HP ProLiant DL360 G7 Server	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the latest service packs and the required software. • System Platform • Communication Manager template	

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the active server

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

   c. In the command line, type **`service_port_access enable`** and press **Enter**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

   - Portable computer access by IP address

     If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.
   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
    - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
    - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

    For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

You back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

   > **Note:**
   >
   > This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.

4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:
     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Connection preservation during an upgrade

When upgrading within the same release, for example, Release 6.0 to Release 6.0.1, you can preserve the following connections:

- The audio portion of many stable telephone calls throughout the course of the upgrade.
- The data transmission between many stable fax, data, or multimedia endpoints.

Communication Manager does not preserve the following connections during an upgrade:

- H.323 IP trunks
- SIP trunks, for example, trunks established for SIP endpoints that use Communication Manager and Session Manager for SIP connections.
- ISDN-BRI trunks or stations
- Unstable calls

  Examples of unstable calls include those that are in the ringing or dialing stage, calls that are on hold, or calls in any state that require control signaling. Unstable calls are dropped, regardless of whether they are carrying voice or data transmissions.
- SAT sessions
- Adjunct links

  Examples of adjunct links include those to a CMS, ASAI, or CDR adjunct, a link to a system printer, or any other links configured using the IP Services screen.

Activating connection preservation during an upgrade

Prerequisites

Log on to the server using System Management Interface.

- If onsite, connect to the Services port on the back of the active server.
- If offsite, log into Communication Manager using the IP address of Communication Manager.

Preserve connections immediately after you perform all standard preupgrade tasks.

1. Under **Server Upgrade**, click **Pre Upgrade Step**.
2. On the Pre Update/Upgrade Step window, click **Continue** to start the preupgrade step.

   The system displays the status of the preupgrade step operations.

Result

The system locks the translations on the active server. This allows the standby server to precisely synchronize translations and preserve connections during the interchange. When the upgrade is complete, the translations are unlocked and the normal synchronization process resumes.

Disconnecting from the server

Unplug the laptop from the services port.

Preupgrade tasks on the standby server

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:

   a. Start an SSH session.

   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type `service_port_access enable` and press **Enter**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type `ip_forwarding disable` and press **Enter**.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

You back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

You back up the data using System Management Interface or System Platform Web Console.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

  Note:
  Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Busying out the standby server

Prerequisites

Log on to System Management Interface of the standby server.

Busyout the standby server.

1. Log in as `craft` or `dadmin`.
2. Under **Server**, click **Busy-Out/Release Server**.
3. Click **Busy Out**.

Upgrade tasks on the standby server

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Upgrading System Platform

Prerequisites

Log on to the System Platform Web console.

Perform the upgrade of System Platform and install the latest service packs or patches.

- System Platform
- System Platform service pack as instructed in Installing patches on page 45.
- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 45.

1. Under **Server Management**, click **Platform Upgrade**.
2. Select the method you adopt for upgrade.
3. Select the file to install for System Platform and click **Select**.
4. Click **Install**.

Next steps

Install the service pack and patches for System Platform as instructed in Installing patches on page 45.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Upgrading the Communication Manager template

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Solution Template**.
2. Select the method you use to access the template.
3. Select the Communication Manager template.
4. Click **Upgrade**.
   The system automatically does the following:
   - Backs up Communication Manager.
   - Installs the new Communication Manager.
   - Restores Communication Manager from the backed up data.

Next steps

Install the service pack and patches for Communication Manager as instructed in Installing patches on page 45.

Verifying Communication Manager operation

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

When the standby server is ready, interchange the roles of the standby and active servers using System Management Interface.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.
   The roles of the active and standby servers changes.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Unplug the laptop from the services port.

Upgrade tasks on the standby server that was active before the interchange

On the server, which was formerly active, and changed to standby state after you interchanged the server roles, perform the following procedures.

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Upgrading System Platform

Prerequisites

Log on to the System Platform Web console.

Perform the upgrade of System Platform and install the latest service packs or patches.

- System Platform
- System Platform service pack as instructed in Installing patches on page 45.
- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 45.

1. Under **Server Management**, click **Platform Upgrade**.
2. Select the method you adopt for upgrade.
3. Select the file to install for System Platform and click **Select**.
4. Click **Install**.

Next steps

Install the service pack and patches for System Platform as instructed in Installing patches on page 45.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.

7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Upgrading the Communication Manager template

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Solution Template**.
2. Select the method you use to access the template.
3. Select the Communication Manager template.
4. Click **Upgrade**.
   The system automatically does the following:
   - Backs up Communication Manager.
   - Installs the new Communication Manager.

- Restores Communication Manager from the backed up data.

Next steps

Install the service pack and patches for Communication Manager as instructed in Installing patches on page 45.

Verifying Communication Manager operation

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay

- **Processes**: okay

3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Unplug the laptop from the services port.

Postupgrade tasks on the active server running Release 6.0.1

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Reset the settings that you recorded Disabling scheduled maintenance on page 37.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
    - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
    - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

    Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

    Note:

    This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

    The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:
     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Postupgrade tasks on the standby server running Release 6.0.1

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

> **Note:**
>
> If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

> **Note:**
>
> If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*

- *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Chapter 3: Upgrading to simplex main/ survivable template

Upgrading the S8500A Server to S8800 Server

Introduction

This section describes the procedure to upgrade S8500A Server running Communication Manager releases 2.0 through 3.x to S8800 Server, HP ProLiant DL360 G7 Server or Dell™ PowerEdge™ R610 Server running Communication Manager Release 6.0.1. The complete list of releases in this range is available on the Avaya Support Web site at www.support.avaya.com.

In this procedure, you replace S8500A Server with an S8800 Server running System Platform and the simplex main/survivable core template (CM_Simplex).

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Creating a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5.
- Installing Communication Manager Release 4.0.5 on S8800 Server and restoring the backed up data from the existing server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.
- Installing System Platform and Communication Manager on S8800 Server.
- Restoring the data set that was created while on Release 4.0.5.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Use this section to upgrade Communication Manager from releases 2.0 through 3.x to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.

- If offsite, log on to the media server using the unique IP address of the media server.

2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.

      The configuration screen appears in your application window.

b. Click **File** and select **Save As**.

c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Print or copy the information from the following screens:

   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**

7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.

8. Click **Administration** > **Server (Maintenance)**.

9. Print or copy the information from the following screens:

   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.

11. On the command line prompt, perform the following:

    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

    c. Enter `almsnmpconf` and record the output.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**

Starting a SAT session

Prerequisites

If you are using Telnet, enable the Telnet service for Communication Manager.

If Telnet is disabled, use SSH to access the SAT.

Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.

- If you are logging on to the server with a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
    - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
    - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - Select **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     1. Select **Specify Data Sets**.
     2. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
3. In the **Download size** field, enter the size of the backup `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
    - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
    - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

    For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp]` or `[all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Preupgrade service packs

You do not need the following preupgrade patches to upgrade S8500A Server running Communication Manager release 2.x to Release 4.0.5 on S8800 server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Service pack for the current software version

You must obtain and activate the latest available service pack for the currently running Communication Manager software version before you proceed with the next upgrade steps. Depending on the release, use one of the following procedures to install the service pack.

Installing service pack updates

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. Enter `cd /var/home/ftp` to access the `ftp` directory.
5. At the prompt, enter `ls -ltr` to list the files in the `ftp` directory.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`.

   Here, *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and takes more than 2 minutes if messaging is enabled. However, wait until the restart or reset process is complete and enter additional commands.

10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. Enter `statapp -c` to view the status of the processes.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP or, if Communication Manager Messaging is installed, 67/67 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.

ii. Click **Yes**.

3. Click **Continue**.

   Note:
   Do not install the preupgrade service pack until instructed.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

  If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

When the backup is complete, the system displays the following message:
`Backup successful`

Caution:

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up files to localhost

Prerequisites

Enable FTP service.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, select **Network Device** and complete the following fields:
   - In the **Method** field, select `FTP`.

- In the **User Name** field, enter `anonymous`.
- In the **Password** field, enter `2` or `@`.
- In the **Host Name** field, enter `localhost`.
- In the **Directory** field, enter `/pub`.

4. Click **Start Backup**.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message: `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.
   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     ```

```
get <name of the backup file>
quit
```

For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

The system closes the ftp session.

8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

The S8500A server continues to provide service until later in the procedure. Do not shut down the S8500A server until instructed.

Upgrade tasks on the S8800 (Release 5.2.1) Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).

- Dell™ PowerEdge™ R610 Server

For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing Communication Manager Release 5.2.1

Prerequisites

- Install the new server in the rack.
- Insert the CD-ROM for Communication Manager Release 5.2.1 into the drive of the server.
- Turn on the server.

1. On your laptop, click **Start** > **Run**.
2. In the Run dialog box, enter `telnet 192.11.13.6` and press `Enter`.

   To navigate on the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install**, highlight **OK** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.
5. When the system prompts you, select SIMPLEX.
6. Select CM only.

   Do not select CM with CMM or CMM stand-alone options.

   The installation process:

   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.

   The installation process takes about 20 minutes. When the server is ready to reboot, the CD/DVD drive door opens and a reminder to check the Avaya Support Site at http://support.avaya.com for the latest software and firmware updates appears on the screen. Remove the CD from the drive.

   The reboot takes about 5–8 minutes. The Telnet session ends automatically.

Checking the reboot progress

1. On the laptop, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
    - The system displays the command line prompt if the cache is cleared.
    - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

    The -t causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Verifying the current software release

1. Under **Server**, click **Software Version**.

    The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
    - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

      This means that Communication Manager Release 4.0.5 is running on the server.
    - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

      This means that Communication Manager Release 5.2.1 is running on the server.

Setting date, time, and time zone

1. Click **Administration** > **Server (Maintenance)**.
2. Under **Server**, click **Server Date/Time**.
3. Change the date, time, and time zone as needed.
4. Click **Submit**.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Using the steps described in this section, you can download the following files:

- The latest available service pack for Communication Manager Release 4.0.5 or Release 5.2.1
- The RFA license for Communication Manager Release 4.0.5 or Release 5.2.1
- Avaya authentication file for Communication Manager Release 4.0.5 or Release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager Release 4.0.5 or Release 5.2.1
- One of the following backup sets:
    - The three-part backup, `os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`
    - Full backup, `full_*.tar.gz`

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     ii. Click **Yes**.
3. Click **Continue**.

   Note:
   Do not install the preupgrade service pack until instructed.

Creating a super-user login

Note:
The craft level login can create a super-user login.

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

   Note:
   Ensure that the customer can change this login, its password, or its permissions.
2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**
   The system displays the Administrator Accounts page.
3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.
   The system displays the Administrator Logins -- Add Login: Privileged Administrator page.
5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

   Note:
   Do not lock the account or set the password to be disabled.
9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.

10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.
    The system informs you the login is added successfully.

Installing the Communication Manager license and authentication files

⚠ **Caution:**

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 111.

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.
   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.
   The system displays a message indicating that the license is installed successfully.
3. Click **Restart CM**.
4. Under **Server**, click **Process Status**.
5. Under **Frequency**, select Display Once.
6. Click **View**.
7. Verify that all operations are `UP`.
8. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.
   The system displays the Authentication File page.
9. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.
   The system displays a message indicating that the authentication file is installed successfully.

Restoring server data

Prerequisites

- Ensure that the license file is valid.

  Note:
  You do not need a license file for survivable core server and survivable remote server.
- Copy the datasets to the server.
- Install the latest service pack for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Depending on the release of Communication Manager of the existing system, the data you restore comes from:

- The three-part backup (os, security, xln) or a full backup
- The backup files copied to the flashcard or the laptop

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - If the backup file is copied to the laptop, click **Local Directory**.

     The fields displays the default directory `/var/home/ftp/pub`. Keep the default directory.
   - If the backup file is copied to the flashcard, click **Local CompactFlash Card**.
3. Click **View**.
4. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
5. Select both **Force** options.
6. Click **Restore**.
7. To view the status of the restore process:
   a. Click **Restore History** and select the file you want to restore.
   b. Click **Status**.
   When the restoration is complete, the system displays the message `backup: 0: restore of <filepath/filename> completed successfully.`

Result

You may lose connectivity between the laptop and the server. Ignore this condition and proceed to the next steps.

Rebooting the server

Use this procedure to reboot the server if the connectivity between the laptop and the server is lost after you restore the data.

Note:

If the connectivity between the laptop and the server is available after you restore the data, use **Server** > **Shutdown Server** on System Management Interface to reboot the server.

1. Press the power control button for several seconds on the front of the server.
   The server turns off.
2. Press the power control button again.
   The server turns on.

Connecting the services laptop to the server

Prerequisites

- Wait for about 5–8 minutes for the system to complete the reboot.
- Verify if ping from the laptop to server is successful.

If the connectivity, ping test, between the laptop and the server is functional, proceed with the section “Accessing the System Management Interface”.

Complete this procedure only if the laptop connected to the services port, the port labeled **2**, is not functional after the reboot.

1. Disconnect the laptop from the Ethernet port labeled **2**.
2. Connect the laptop to the Ethernet port labeled **4**.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.

   ii. The system displays the status as the update progresses. The system automatically reboots, if required.
   iii. Click **Yes**.
3. Click **Continue**.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up files to localhost

Prerequisites

Enable FTP service.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, select **Network Device** and complete the following fields:
   - In the **Method** field, select `FTP`.
   - In the **User Name** field, enter `anonymous`.

- In the **Password** field, enter `2` or `@`.
- In the **Host Name** field, enter `localhost`.
- In the **Directory** field, enter `/pub`.

4. Click **Start Backup**.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message: `Backup successful`

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.
   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget migration-60*
     y
     quit
     ```
   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     ```

```
get <name of the backup file>
quit
```

For example, `migration-60_cmserver_172731_20100516.tar.gz`.

The system closes the ftp session.

8. To confirm that the backup file, for example, `migration-60*.tar.gz` is present, enter `dir migration*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Upgrade tasks on the S8800 (Release 6.0.1) Server

Turning on the server

Prerequisites

Do not connect the server to the network.

1. Insert the System Platform DVD into the CD/DVD drive of the server.
2. Turn on the server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:

  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled

for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

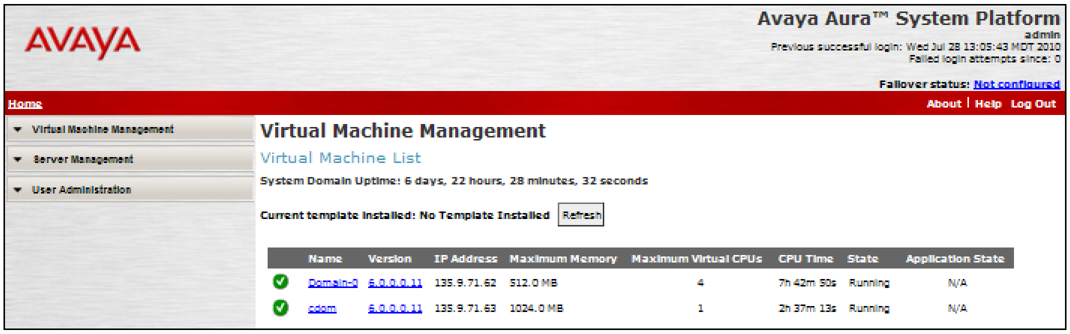
Note:

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.
   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying the upgrade dataset from the laptop to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.

5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.
   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Completion tasks on the S8500A Server

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Postupgrade tasks on the S8800 (Release 6.0.1) Server

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     i. Click **Change**.
     ii. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:
    - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
    - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
    - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

    Note:
    Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500-Series Server to S8800 Server

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 on S8500B or S8500C Server to Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server or Dell™ PowerEdge™ R610 Server.

In this procedure, you replace the S8500B or S8500C Server by an S8800 Server, Dell™ PowerEdge™ R610 Server or HP ProLiant DL360 G7 Server running System Platform and the simplex main/survivable core template (CM_Simplex).

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8500B or S8500C Server to Communication Manager Release 4.0.5 or Release 5.2.1 first.
    - For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
    - For S8500A server, see *Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603445).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.0.1.
3. Perform the upgrade to Release 6.0.1 as described in this section.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist for server upgrades

You need the following additional documentation:

✔	Task	Description
	Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603444.	Provides instructions for installing the S8800 Server for Communication Manager.

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager, 03-603558.	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the S8500 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.
      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**

- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging in from a laptop directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.

- If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.
   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:

- If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
- If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

✱ **Note:**

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.
   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
    - If Communication Manager Messaging is not enabled:

      Select **Full Backup**.

      The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

      Note:
      For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

      - **Avaya Call Processing (ACP) Translations**
      - **Server and System Files**
      - **Security Files**
    - If Communication Manager Messaging is enabled:
        1. Select **Specify Data Sets**.
        2. Select the following check boxes:
            - **Avaya Call Processing (ACP) Translations**
            - **Server and System Files**
            - **Security Files**
            - **Communication Manager Messaging (CMM)**

              Select **Translations, Names, and Messages**.
        3. In the **Download size** field, enter the size of the backup `.tar` file.

           There could be more than one `.tar` file if the backup size is large.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
    - **User Name**

- **Password**
- **Host Name**. Enter the host IP address.
- **Directory**

  When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.

5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.

The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**

- **Directory**

  The backup location must be a server on the customer LAN.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager

Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.

10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

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

    ```
    Backup successful
    ```

    > ⚠ **Caution:**
    >
    > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
    - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

    The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier.

When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the cables

1. Disconnect the laptop from the Services port.
2. Label and disconnect the power cord(s) from the power supply at the back of the server.
3. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
4. Disconnect the power cord from the SAMP at the back of the server.

Removing the server from the rack

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Upgrade tasks on the S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:

  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Communication Manager Messaging file.

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

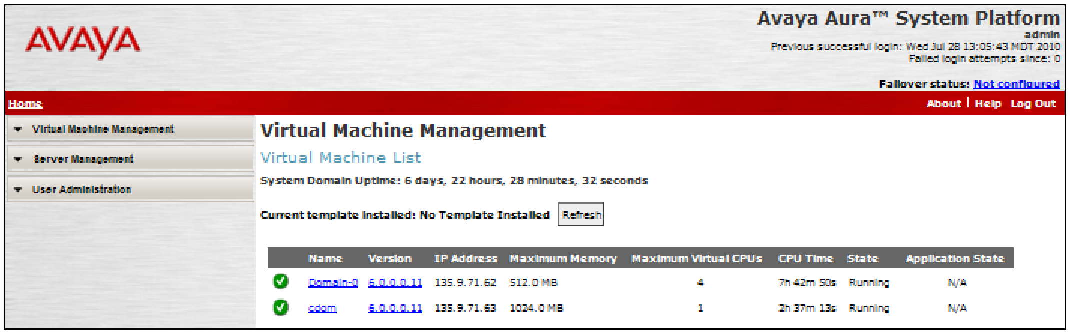
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.

4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
   a. Select **Miscellaneous** > **Messaging Software**.
   The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.
   The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

Important:

Communication Manager Messaging processes are stopped during RFU installation.

If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
    a. In the **Name** field, enter `tmp`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
    This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
    a. Record the value of the **Far-end Node Name** field.

    You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
    b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
    a. In the **Name** field, enter `msgserver`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
    a. In the **Far-end Node Name** field, enter `msgserver`.
    b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

    Remove the entries from the **Name** and **IP Address** fields and submit the form.

    This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8510 Server to S8510 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager to Release 6.0.1 running System Platform and the simplex main/survivable core template (CM_Simplex) for existing Communication Manager on S8510 Server.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

You can reuse the existing server. However, if the current disks are of 146GB memory, perform the following additional tasks:

- Increase the memory
- Remove the SAMP
- Add a third hard drive, only if the current disks are of the type SAS with 146GB memory
- Reconfigure to RAID 5, only if you add a third hard disk drive

For servers that you can upgrade directly to Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.0.1 on:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

      If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
    - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.
    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**
    - **Set Identities**
    - **Configure Interfaces**
    - **Set DNS/DHCP**
    - **Set Static Routes**
    - **Configure Time Server**
    - **Server Access**
    - **Server Date/Time**
    - **Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
    - If Communication Manager Messaging is not enabled:

        Select **Full Backup**.

        The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

        Note:
        For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
    - If Communication Manager Messaging is enabled:
        1. Select **Specify Data Sets**.
        2. Select the following check boxes:
            - **Avaya Call Processing (ACP) Translations**
            - **Server and System Files**
            - **Security Files**
            - **Communication Manager Messaging (CMM)**

                Select **Translations, Names, and Messages**.
        3. In the **Download size** field, enter the size of the backup `.tar` file.

            There could be more than one `.tar` file if the backup size is large.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**. Enter the host IP address.
    - **Directory**

    When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.

5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking hardware on the server

To verify if you need to install the additional hard disk drive on the server to support Communication Manager. RAID configuration on the server:

1. Log on to the System Management Interface and select **Administration** > **Server (Maintenance)**.
2. Under **Server Configuration**, select **Display Configuration**.
3. Under **Disk devices**, verify the type and the number of hard disk drives (HDD) installed on the system. If the system displays:
   - SAS 146GB, you need to add a third SAS 146GB hard disk drive. You also need to convert RAID 1 to RAID 5.
   - SATA, do not add a third hard disk drive.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.

4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

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

    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
    - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

    The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

    There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**

8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    > ⚠ **Caution:**
    >
    > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Remove the front bezel from the S8510 server

> ⚠ **Caution:**
>
> Wear an antistatic wrist ground strap whenever you handle any S8510 server components. Connect the strap to an approved ground such as an unpainted metal surface. Also, place the hard drive on an antistatic mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

1. If locked, unlock the bezel with the system key.

Security alert:

If the front bezel is locked, ensure that you lock it when you are finished with this replacement procedure.

2. Press the left tab of the bezel and rotate the left end away from the server.
3. Release the right end of the bezel and pull it away from the server.
4. Set the bezel aside.

Disconnecting the cables

1. Label and disconnect the power cord(s) from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
3. Disconnect the power cord from the SAMP at the back of the server.
4. Disconnect the USB modem cable from the USB port on the SAMP at the back of the server.
5. Disconnect the LAN connection, if used from the Ethernet port on the SAMP at the back of the server.

Removing the server from the rack

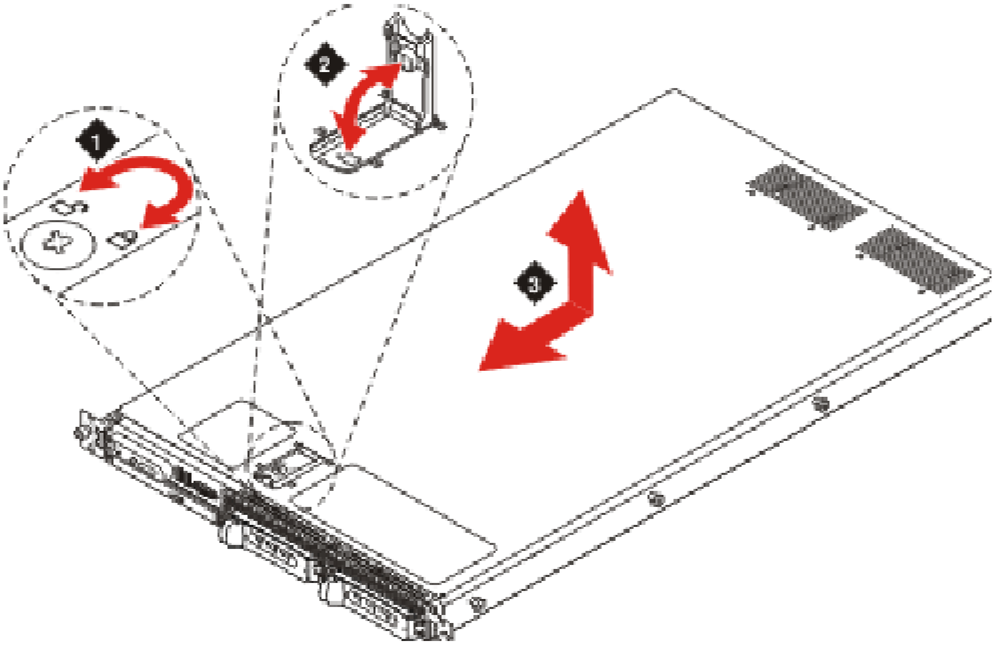
Prerequisites

⚠ **Caution:**

Ensure that the power is completely removed from the server: power cords must be detached from the power source and the SAMP.

1. Loosen the captive screws on both sides of the server.
2. Slide the server clear of the rails
3. Release the rail lock by pushing the lever in as you slide the server out of the rack.

Removing the cover of the S8510 Server



1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver (Figure 1).
2. Lift the latch up to unlock (Figure 2).
3. Slide the cover back and lift straight up to remove (Figure 3).

Adding the memory modules

Caution:
Ensure that you wear electrostatic wrist ground strap on your bare wrist.

1. Remove the protective cover over the memory modules.
2. Insert the new memory modules.

Removing the SAMP

⚠ **Caution:**

The SAMP has a separate power source from the server's. You must remove all power from the server and the SAMP card before starting this procedure.

⚠ **Warning:**

Take precautions against electrostatic discharge. Wear a wrist strap connected to an approved ground.

The SAMP card resides in a PCI expansion card riser at the rear of the server.

1. Lift the release latches on the PCI expansion card riser.
2. Disconnect the cable assembly from the SAMP. Set the cable aside; you will not reuse the cable but will return it to Avaya with the SAMP.
3. Remove the SAMP card by pulling it gently out of the expansion slot in the riser assembly.
4. Remove the ribbon cable from the motherboard.

Next steps

Insert a face plate in the empty slot from where you removed the SAMP card.

This prevents any dust from entering the server through the empty slot.

Adding a third hard drive

Prerequisites

Check if you need the third hard disk drive. See Checking hardware on the server on page 178.

Remove the front bezel and cover to add the hard drive.

1. Pinch together the two tabs of the drive carrier release handle.
2. Open the carrier release handle.
3. Insert the hard drive in to the slot and push it inside until it is seated.
4. Close the hard drive carrier handle to lock the hard drive in place.

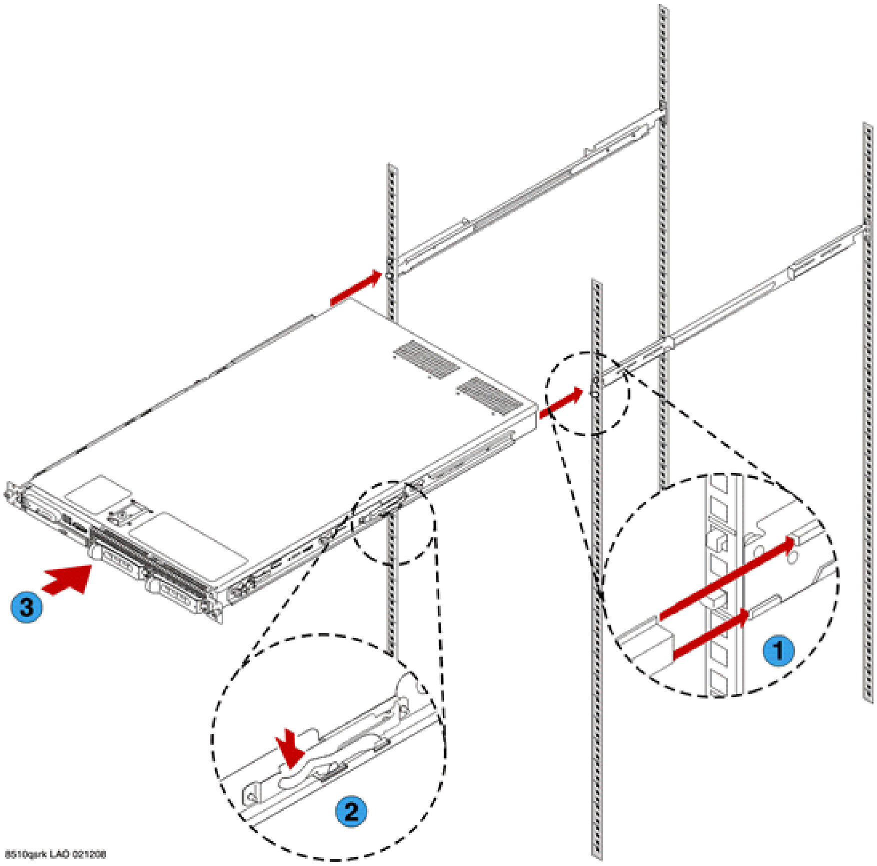
Replacing the cover on S8510 server

1. Place the cover on top of the server, aligning it with the J hooks on the sides.
2. Slide the cover forward.
3. Push the latch down to lock.
4. Rotate the latch release lock clockwise to secure the cover.

Installing the server in the rack

Prerequisites

The rails must be attached to the server and the rack before installing the server in the rack. If the server is being installed in a cabinet, remove the doors, following the cabinet manufacturer's instructions.



Next steps

If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Replacing the front bezel

1. Seat the right end of the bezel in the notch on the right front of the server chassis.
2. Press the left end of the bezel into place until the tab locks in place.
3. If the bezel was originally locked, lock the bezel with the system key.

Converting the disk array to RAID 5

Prerequisites

CD comcoded 700500415

Important:

This process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

1. Insert the CD comcoded 700500415 into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following messages:

   ```
   2 Hard Drives Found, Applying Avaya RAID 1 Configuration & Settings 3 Hard
   Drives Found, Applying Avaya RAID 5 Configuration & Settings 4 Hard Drives
   Found, Applying Avaya RAID 5 Configuration & Settings
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and rerun the configuration tool. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:

  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Communication Manager Messaging file.

  Note:

  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

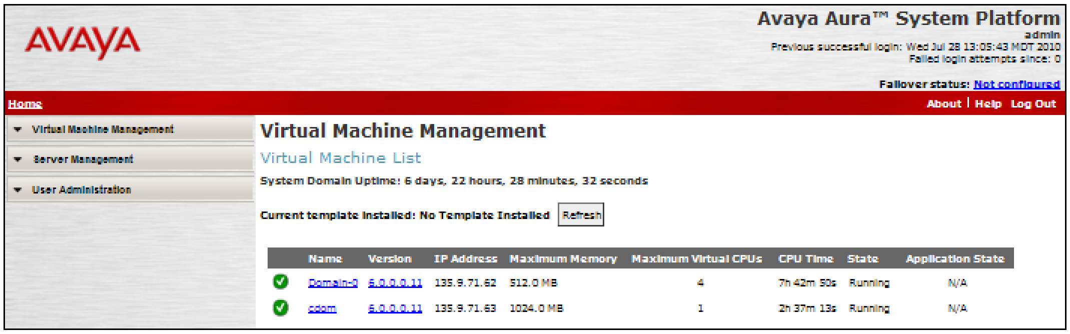
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.

3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two

ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.

4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   > **Important:**
   > Communication Manager Messaging processes are stopped during RFU installation.
   >
   > If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.
   >
   > Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
    1. In the **Name** field, enter `tmp`.
    2. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
       This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
    1. Record the value of the **Far-end Node Name** field.

       You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
    2. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
    1. In the **Name** field, enter `msgserver`.
    2. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
    1. In the **Far-end Node Name** field, enter `msgserver`.
    2. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.

5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     i. Click **Change**.
     ii. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

Note:

Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8800 Server to S8800 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager running on S8800 Server from Release 5.2.1 to Release 6.0.1. In this procedure, you reuse the S8800 Server and install System Platform and the simplex main/survivable core template on the server.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following additional tasks to reuse the existing server:

- Increase the memory
- Add a third hard drive
- Update the uEFI firmware
- Reconfigure the RAID controller to support RAID 5
- Update the uEFI settings

> **Note:**
>
> For instructions to update the uEFI firmware and uEFI settings, download the release notes from the Avaya Support Web site at http://support.avaya.com.

For more information see, the *Avaya S8800 Migration Kit*.

Use this section to upgrade:

- the main server
- the survivable core server (formerly enterprise survivable servers)

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade.

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager template	
	Verify that you have all the necessary equipment onsite, for example: • Hard disk drive • Memory module • Services laptop and crossover cable • Electrostatic wrist ground strap and mat	For the list of required equipment, see *Avaya Migration Kit.*
	Obtain the CD to update the uEFI firmware using one of the following ways: • Order the uEFI firmware CD • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.	
	Obtain the RIAD 5 firmware CD	

✔	Task	Description
	Obtain the CD to update the uEFI settings using one of the following ways: • Order the uEFI settings CD • Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Documentation checklist for server upgrades

You need the following additional documentation:

✔	Task	Description
	Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603444.	Provides instructions for installing the S8800 Server for Communication Manager.
	Installing and Configuring Avaya Aura™ Communication Manager, 03-603558.	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**
    - **Set Identities**
    - **Configure Interfaces**
    - **Set DNS/DHCP**
    - **Set Static Routes**
    - **Configure Time Server**
    - **Server Access**
    - **Server Date/Time**
    - **Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging in from a laptop directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

     > **Note:**
     > For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:
     >
     > - **Avaya Call Processing (ACP) Translations**
     > - **Server and System Files**
     > - **Security Files**

   - If Communication Manager Messaging is enabled:

     i. Select **Specify Data Sets**.

     ii. Select the following check boxes:

       - **Avaya Call Processing (ACP) Translations**
       - **Server and System Files**
       - **Security Files**
       - **Communication Manager Messaging (CMM)**

         Select **Translations, Names, and Messages**.

     iii. In the **Download size** field, enter the size of the backup `.tar` file.

       There could be more than one `.tar` file if the backup size is large.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.

5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > ⚠ **Caution:**
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Verifying the hardware on the server

Verify the memory, hard drive, and RAID configuration on the existing server:

1. Log on to System Management Interface and select **Administration** > **Server (Maintenance)**.
2. Under **Server Configuration**, select **Display Configuration**.
3. Under **Disk devices**, verify if the system has three 146GB hard disk drives. If the system does not have three disk drives, install a disk drive on the server later when you are instructed to do so.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.

4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

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

    ```
    Backup successful
    ```

    > ⚠ **Caution:**
    >
    > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
   - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**

8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    > ⚠ **Caution:**
    >
    > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the cables

1. Label and disconnect the power cord(s) from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server cover

Prerequisites

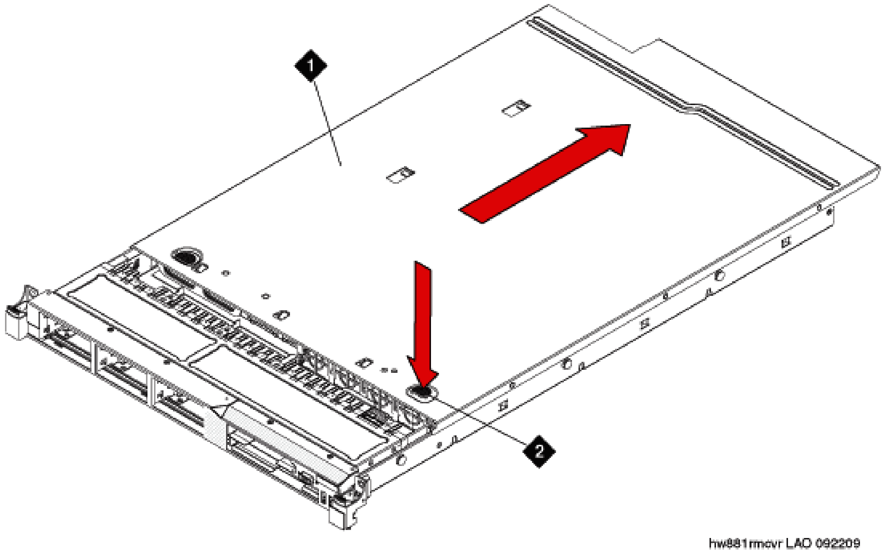
Before you disconnect the server from the power source, make a note of which LEDs are lit, including the LEDs that are lit on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs are not lit when the power source is removed.

Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
    a. Turn off the server and all attached devices.
    b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

   Important:

   For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

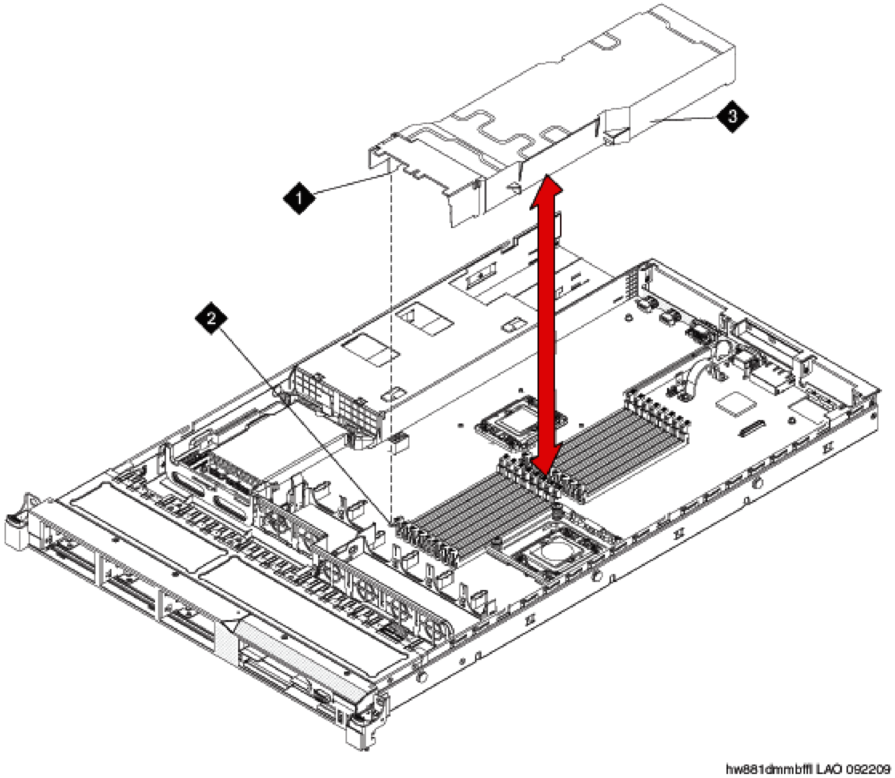
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Grasp the DIMM air baffle and lift the air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Prerequisites

Remove the DIMM air baffle.

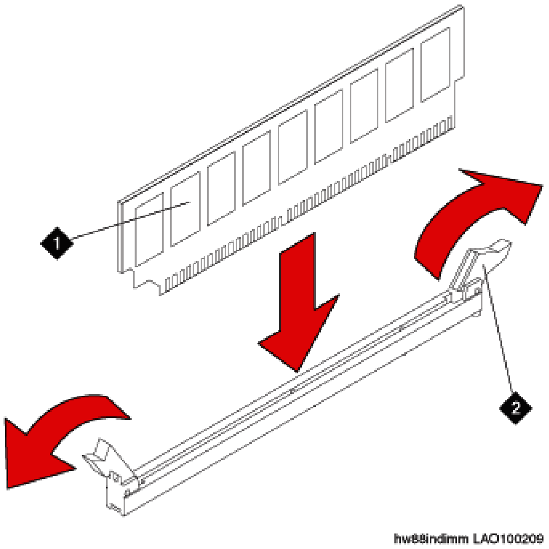
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.
   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

Important:

If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.

7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.
    When you install or remove memory modules, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

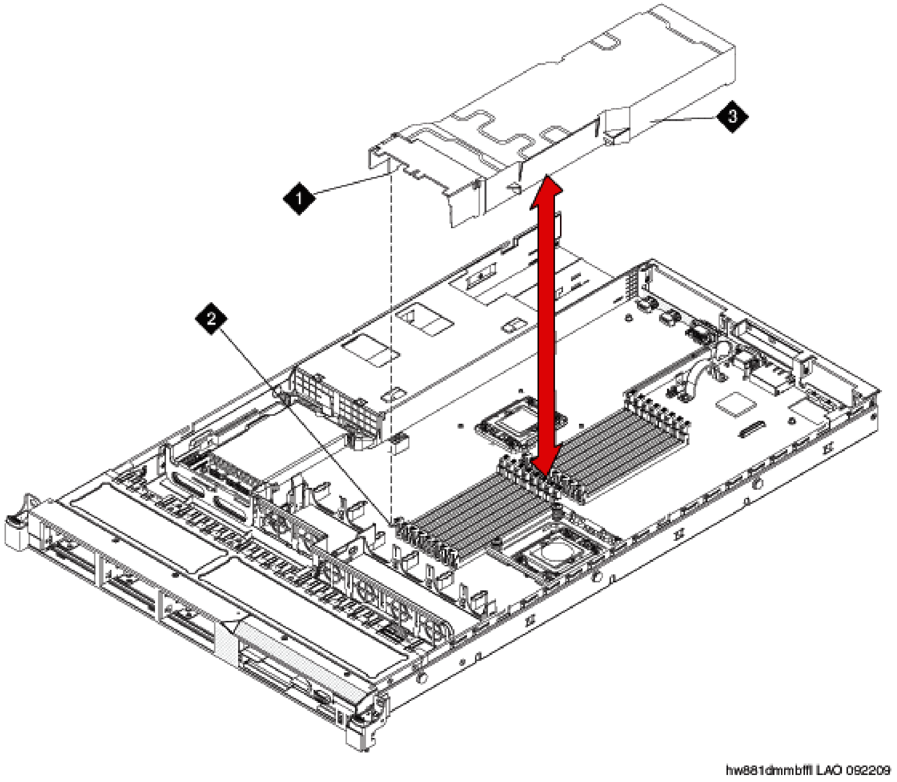
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

Prerequisites

If replacing an existing hard drive, remove the hard drive that you want to replace.

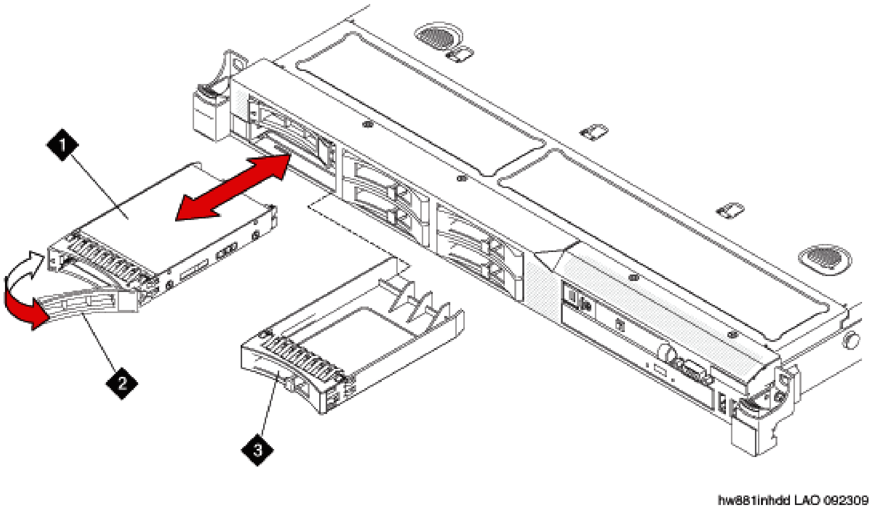
Important:

To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. If the amber LED remains lit, the drive is faulty and must be replaced.

Updating S8800 server firmware

Prerequisites

- Obtain the CD for uEFI firmware. You must either order the CD or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:
If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Prerequisites

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:
The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.
2. Verify that the system configures the RAID successfully. The screen must display the following message:
   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration &
   Settings....
   ```
   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server,

reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Next steps

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

Prerequisites

- Obtain the CD for uEFI settings of S8800 Server. You may order the CD, or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Communication Manager Messaging file.

  Note:
  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type `service_port_access enable` and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

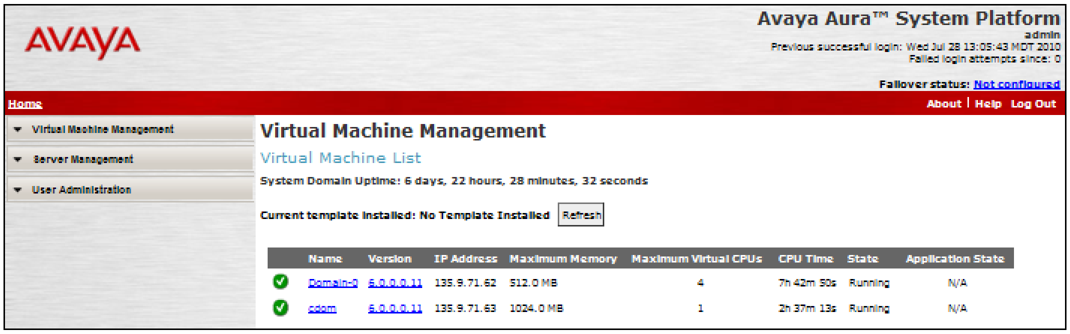
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Fallover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
    The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
    - File(s) to download from the machine I'm using to connect to the server.
    - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the RFU.
    - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:
   Communication Manager Messaging processes are stopped during RFU installation.

If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.

   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.

4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system

Prerequisites

Start a SAT session.

Enter `list station` and verify that the stations listed after the upgrade are the same as the stations listed before the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Reset the settings that you recorded Disabling scheduled maintenance on page 37.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp]` or `[all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.

- Enter `save translation`.

  Note:

  If this operation fails, follow the escalation procedures before you continue with the next step.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Upgrading DEFINITY SI or R Server to the S8800 Server

Introduction

This section describes the procedure to upgrade the following servers to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server or Dell™ PowerEdge™ R610 Server:

- DEFINITY SI Server in an SCC1 or an MCC1
- DEFINITY R Server in an MCC1

In this procedure:

- You discard:
    - All port networks (SCCs or MCCs)
    - SI or R processor circuit pack
- You install:
    - A G650 Media Gateway and move the supported circuit packs to the media gateway.
    - An S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex main/survivable core template (CM_Simplex).

The simplex main/survivable core main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing translation file on Communication Manager Release 6.0.1.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

This upgrade affects service. When you turn off the PPN stack to replace the cabinet as part of the upgrade process, the system drops all calls. Service returns when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following server, as appropriate: - S8800 Server	

✔	Task	Description
	- Dell™ PowerEdge™ R610 Server - HP ProLiant DL360 G7 Server • G650 Media Gateway • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP or later C-LAN	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	Installing the Avaya G650 Media Gateway (03-300685)	Provides instructions for installing and configuring the G650 Media Gateway.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PNs to prepare the DEFINITY system for upgrade. The changing or upgrading the hardware includes:

- Changing TN2182 Tone Clock and maintenance circuit packs for TN2312BP IP Server Interfaces (IPSI) and new TN779D maintenance circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service. However, duplex-reliability configurations encounter short service interruptions when you change the tone-clock circuit pack is in IPSI-controlled PNs.

Server and IPSI cable connections

Each IPSI circuit pack must have a CAT5 cable that connects to the customer network. Cables for IPSIs are located in PN carrier A. If the system has a duplicated bearer network, the cables for IPSIs are located in PN carrier B.

In duplex configurations, each server is connected to the customer network that comprise control network A (CNA). If this system has duplicated IPSIs, each server is connected to the customer network that comprise control network B (CNB).

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Replacement of circuit packs

All PNs receive IPSI circuit packs. The TN2312BP IPSI circuit pack replaces the existing TN2182 Tone Clock circuit pack and terminates control communication with the servers. Flat ribbon cables run between the IPSIs and the maintenance circuit pack. These ribbon cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit packs, program static IP addresses into the IPSIs.

You can complete this stage at any time before the cutover. The tone clock and the IPSI circuit packs are hot swappable, and you replace the circuit packs in the existing DEFINITY system without the need to turn off the power.

The IPSI circuit pack provides the same functionality as the tone clock circuit pack. You perform the following tasks before the cutover:

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSIs are working as tone clocks in the existing system.
- Test the connectivity between the server and the IPSI.
- Reinstall the IPSIs in the new carriers after you install the carriers.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Prerequisites

A cross-over cable to connect your services laptop directly to the processor.

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603444).
- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled

for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   1. Start an SSH session.
   2. Log in to System Domain (Domain-0) as admin.
   3. In the command line, type `service_port_access enable` and press **Enter**.
2. To disable IP forwarding:
   1. Start an SSH session.
   2. Log in to System Domain (Domain-0) as admin.
   3. In the command line, type `ip_forwarding disable` and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

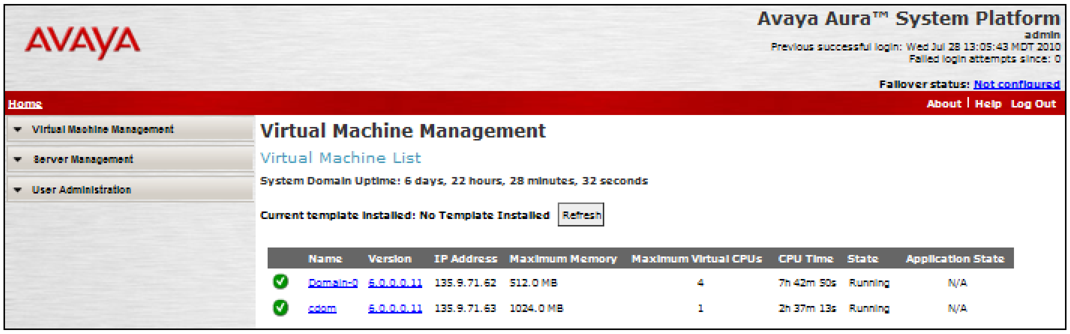
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

> **Note:**
> This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two

ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the translations

Prerequisites

Log in to System Management Interface.

Use this procedure to restore translations only on the main server. When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

1. Under **Administration**, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

      Important:
      If the server is not connected to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:
   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the Restore status.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
    The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
    - File(s) to download from the machine I'm using to connect to the server.
    - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the RFU.

- Enter the URL to download the RFU and enter the host name and domain name of the proxy server.

5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.

   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.
      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.

6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
    - If the information is correct, proceed with Step 3.
    - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

    For more information, see About subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

    Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing G650 Media Gateway in the rack

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.

6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.
   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
   d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.
   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
   d. Enter `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.
4. For G650, if the maintenance function is used:
   1. Connect one end of the serial maintenance cable to the DB9 connector on the IPSI adapter.
   2. Connect the other end to the Emergency Transfer panel to provide 1 alarm output and 2 alarm inputs.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.

4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack` *`n`*, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Port network circuit packs

Because you do not reuse the PPN after the upgrade, you must:

- Relocate the port network circuit packs to a new G650 Media Gateway.
- Remove all port network circuit pack translations related to the PPN. The STS group manages the translation changes necessary for this upgrade.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface` *`PNnumber`*, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to `y`.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to `y`.
4. Verify that all the other fields are populated.

5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you might also need to adjust the administration of the network regions. Your planning documents might provide information about changes to network regions. For more information on how to administer network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit packs

Prerequisites

Start a SAT session.

Complete Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6

- DiffServ: 46

3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

The default is **none**.

Removing fiber-related administration

Prerequisites

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Administering PN synchronization

Prerequisites

Open a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network` *n*, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

The system displays a list of all the cabinets and the PNs that the cabinets contain under **Circuit Packs Available for Synchronization**.

5. Obtain a location for the synchronization source circuit pack from the list under **Circuit Packs Available for Synchronization** for **Primary** and **Secondary** fields. Ensure that you choose a working synchronization source.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, add another synchronization-source circuit pack location in the **Secondary** field.
8. Press **Submit**.

   Wait about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization-switch all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must show `PASS` in the **Results** field. If the **Results** field does not show `PASS`, you must troubleshoot the synchronization error.

Completion tasks on the cabinet

Disconnecting from the server

Unplug the laptop from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

1. Remove the fiber cables that connect the following circuit packs in the PNs:

- For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
- For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B

2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Cutover to the server control

Because you do not reuse the PPN, you relocate the port network circuit packs to G650 Media Gateway.

When you relocate the circuit packs to the media gateway and you turn on the power, you want to cut over to have the new server control the existing PNs. The server can be an S8800 Server, Dell™ PowerEdge™ R610 Server or an HP ProLiant DL360 G7 Server. To cut over to the server, you must enable the IPSIs on the IP Server Interface (IPSI) System Parameters screen.

This stage affects service momentarily while the CSS comes up and the calls are load balanced across the IPSIs throughout the port networks.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   ⚠ **Caution:**

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

   Note:

   You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or the customer wants to minimize out-of-service time.
4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on the new server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.

3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

Note:

Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Chapter 4: Upgrading to simplex survivable remote template

Upgrading the S8500A Server to S8800 Server

Introduction

Use this procedure to upgrade S8500A Server running Communication Manager releases 2.0 through 3.x to S8800 Server, HP ProLiant DL360 G7 Server or Dell™ PowerEdge™ R610 Server running Communication Manager Release 6.0.1. The complete list of releases in this range is available on the Avaya Support Web site at www.support.avaya.com.

The procedure requires you to replace the S8500A Server configured as survivable remote processor, formerly Local Survivable Processor (LSP) with an S8800 Server running System Platform and the survivable remote template (CM_SurvRemote).

The upgrade procedure involves:

- Recording the configuration information from the existing S8500A Server in the upgrade worksheet.
- Shutting down the S8500A Server and installing the S8800 Server.
- Installing System Platform and Communication Manager survivable remote template on S8800 Server.
- Configuring Communication Manager to be the survivable remote.

The upgrade procedure synchronizes translations and user accounts from the main Communication Manager server to the survivable remote server. You require a new authentication file for Communication Manager Release 6.0.1 configured as survivable remote server.

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.
6. Print or copy the information from the following screens:
    - **Set Identities**
    - **Configure Interfaces**

- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**

7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
    - **Alarms** > **SNMP Agents**
    - **Alarms** > **SNMP Traps**
    - **Server** > **Server Date/Time**
    - **Security** > **Server Access**
    - **Miscellaneous** > **CM Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

    c. Enter `almsnmpconf` and record the output.

Recording the scheduled backups

Record the backup scheduled for the existing server. You must submit the scheduled backups after the upgrade.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Record the details of any backup schedules.

   You will submit these scheduled backups after the upgrade on the new server running Communication Manager Release 6.0.x.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
    - **Telnet Server (23)**
    - **SAT (Telnet 5023)**

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:

- For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
    - **Avaya Call Processing (ACP) Translations**
    - **Server and System Files**
    - **Security Files**
- For Communication Manager release 3.0 or later, select **Full Backup**.

3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message: `Backup successful`

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
    - Select **Full Backup**.
    - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
        i. Select **Specify Data Sets**.
        ii. Select the check boxes:
            - **Avaya Call Processing (ACP) Translations**
            - **Server and System Files**
            - **Security Files**
3. In the **Download size** field, enter the size of the backup `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.

5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Upgrade tasks on the S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

c. In the command line, type `ip_forwarding disable` and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

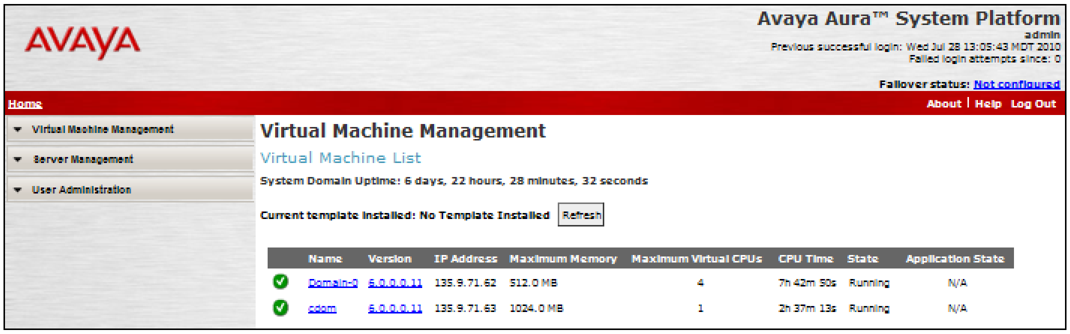
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Configuring the alarming information

Prerequisites

Log on to System Management Interface.

Configure the information provided in the worksheet available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431).

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:
   1. Under **Server**, click **Shutdown Server**.
   2. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Submitting the scheduled backups

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. On the Schedule Backup Web page, select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500-Series Server to S8800 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 4.0.5 or Release 5.2.1 on S8500B or S8500C server to Release 6.0.1.

In this upgrade procedure, you replace the S8500B or S8500C server by an S8800 Server, Dell™ PowerEdge™ R610 Server or HP ProLiant DL360 G7 Server running System Platform and the simplex survivable remote template.

The simplex survivable remote template supports:

- Communication Manager (without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager release 6.0.1.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8500 Server to Communication Manager Release 4.0.5 or Release 5.2.1.
   - For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
   - For S8500A server, see *Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603445).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.0.1.
3. Perform the upgrade to Release 6.0.1 as described in this section.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist for server upgrades

You need the following additional documentation:

✔	Task	Description
	Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603444.	Provides instructions for installing the S8800 Server for Communication Manager.
	Installing and Configuring Avaya Aura™ Communication Manager, 03-603558.	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)

4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the S8500-Series Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.
      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
    - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
    - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.
   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:

- If Communication Manager Messaging is not enabled:

  Select **Full Backup**.

  The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

  Note:

  For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
- If Communication Manager Messaging is enabled:

  i. Select **Specify Data Sets**.

  ii. Select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
  - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.

  iii. In the **Download size** field, enter the size of the backup `.tar` file.

  There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.

6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:

- **User Name**
- **Password**
- **Host Name**
- **Directory**

The backup location must be a server on the customer LAN.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

5. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the cables

1. Disconnect the laptop from the Services port.
2. Label and disconnect the power cord(s) from the power supply at the back of the server.

3. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
4. Disconnect the power cord from the SAMP at the back of the server.

Removing the server from the rack

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Upgrade tasks on the S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled

for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

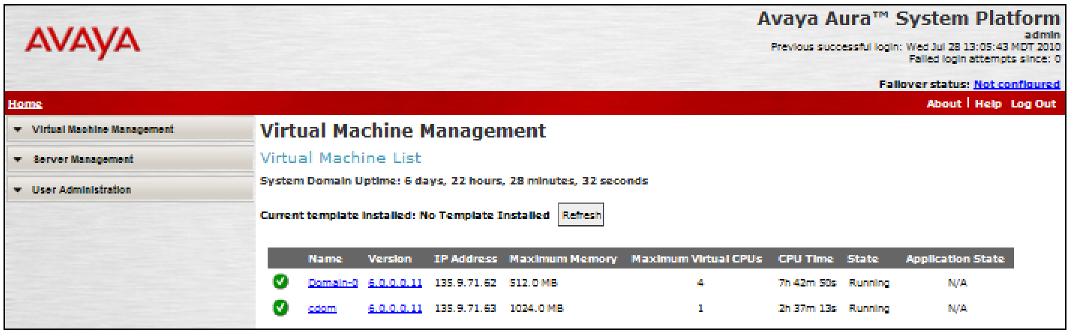
Note:

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   > **Note:**
   > If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

> **Note:**
>
> If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

> **Note:**
>
> You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.

- If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

  Important:

  If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:

i. Click **Change**.

ii. On the Change Current Schedule Web page, click **Change Schedule**

- To remove the schedule backup, click **Remove**.

  The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:
     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Upgrading the S8510 Server to S8510 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager to release 6.0 running System Platform and the simplex survivable remote template for existing Communication Manager on S8510 server.

The simplex survivable remote template supports:

- Communication Manager (without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager release 6.0.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager release 6.0.

You can reuse the existing server. However, you need to perform the following additional tasks:

- Increase the memory
- Remove the SAMP
- Add a third hard drive, only if the current disks are of SAS with 146GB memory.
- Reconfigure to RAID 5, only if you add a third hard disk drive.

For servers that you can upgrade directly to release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:

a. Right-click and select **Paste**.

   The configuration screen appears in your application window.

b. Click **File** and select **Save As**.

c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging in from a laptop directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.
   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:

  i. Select **Specify Data Sets**.

  ii. Select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
  - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.

  iii. In the **Download size** field, enter the size of the backup `.tar` file.

  There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.

ii. Wait until the system displays the message, `... unpacked successfully`.

- If the status of the update file you want to activate is unpacked:

  i. Select the **Update ID** and click **Activate**.

  ii. The system displays the status as the update progresses. The system automatically reboots, if required.

  iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Remove the front bezel from the S8510 server

⚠ **Caution:**

Wear an antistatic wrist ground strap whenever you handle any S8510 server components. Connect the strap to an approved ground such as an unpainted metal surface. Also, place the hard drive on an antistatic mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

1. If locked, unlock the bezel with the system key.

   ❗ **Security alert:**

   If the front bezel is locked, ensure that you lock it when you are finished with this replacement procedure.
2. Press the left tab of the bezel and rotate the left end away from the server.

3. Release the right end of the bezel and pull it away from the server.
4. Set the bezel aside.

Disconnecting the cables

1. Label and disconnect the power cord(s) from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.
3. Disconnect the power cord from the SAMP at the back of the server.
4. Disconnect the USB modem cable from the USB port on the SAMP at the back of the server.
5. Disconnect the LAN connection, if used from the Ethernet port on the SAMP at the back of the server.

Removing the server from the rack

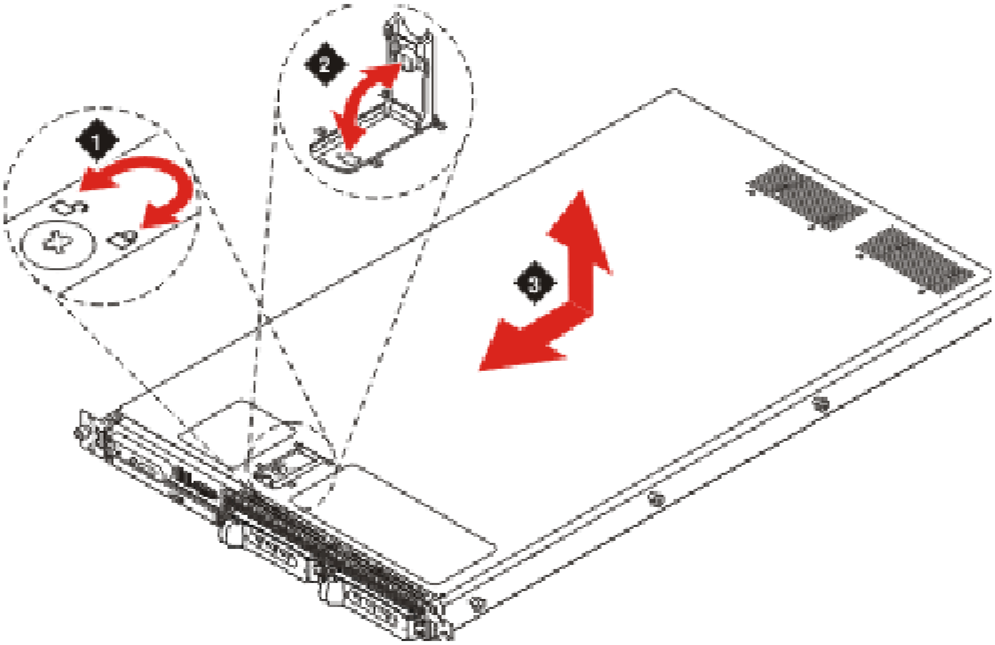
Prerequisites

⚠ **Caution:**

Ensure that the power is completely removed from the server: power cords must be detached from the power source and the SAMP.

1. Loosen the captive screws on both sides of the server.
2. Slide the server clear of the rails
3. Release the rail lock by pushing the lever in as you slide the server out of the rack.

Removing the cover of the S8510 Server



1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver (Figure 1).
2. Lift the latch up to unlock (Figure 2).
3. Slide the cover back and lift straight up to remove (Figure 3).

Adding the memory modules

Caution:
Ensure that you wear electrostatic wrist ground strap on your bare wrist.

1. Remove the protective cover over the memory modules.
2. Insert the new memory modules.

Removing the SAMP

⚠ **Caution:**

The SAMP has a separate power source from the server's. You must remove all power from the server and the SAMP card before starting this procedure.

⚠ **Warning:**

Take precautions against electrostatic discharge. Wear a wrist strap connected to an approved ground.

The SAMP card resides in a PCI expansion card riser at the rear of the server.

1. Lift the release latches on the PCI expansion card riser.
2. Disconnect the cable assembly from the SAMP. Set the cable aside; you will not reuse the cable but will return it to Avaya with the SAMP.
3. Remove the SAMP card by pulling it gently out of the expansion slot in the riser assembly.
4. Remove the ribbon cable from the motherboard.

Next steps

Insert a face plate in the empty slot from where you removed the SAMP card.

This prevents any dust from entering the server through the empty slot.

Adding a third hard drive

Prerequisites

Check if you need the third hard disk drive. See Checking hardware on the server on page 178.

Remove the front bezel and cover to add the hard drive.

1. Pinch together the two tabs of the drive carrier release handle.
2. Open the carrier release handle.
3. Insert the hard drive in to the slot and push it inside until it is seated.
4. Close the hard drive carrier handle to lock the hard drive in place.

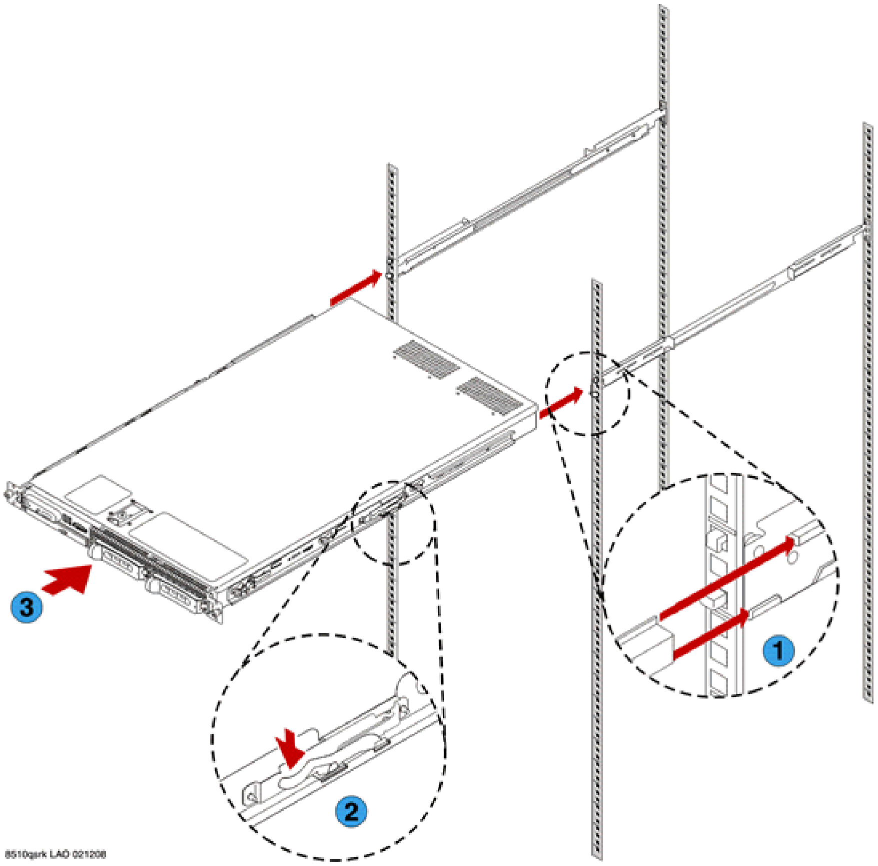
Replacing the cover on S8510 server

1. Place the cover on top of the server, aligning it with the J hooks on the sides.
2. Slide the cover forward.
3. Push the latch down to lock.
4. Rotate the latch release lock clockwise to secure the cover.

Installing the server in the rack

Prerequisites

The rails must be attached to the server and the rack before installing the server in the rack. If the server is being installed in a cabinet, remove the doors, following the cabinet manufacturer's instructions.



Next steps

If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Replacing the front bezel

1. Seat the right end of the bezel in the notch on the right front of the server chassis.
2. Press the left end of the bezel into place until the tab locks in place.
3. If the bezel was originally locked, lock the bezel with the system key.

Converting the disk array to RAID 5

Prerequisites

CD comcoded 700500415

Important:

This process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

1. Insert the CD comcoded 700500415 into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following messages:

   ```
   2 Hard Drives Found, Applying Avaya RAID 1 Configuration & Settings 3 Hard
   Drives Found, Applying Avaya RAID 5 Configuration & Settings 4 Hard Drives
   Found, Applying Avaya RAID 5 Configuration & Settings
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server, reboot the server and rerun the configuration tool. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

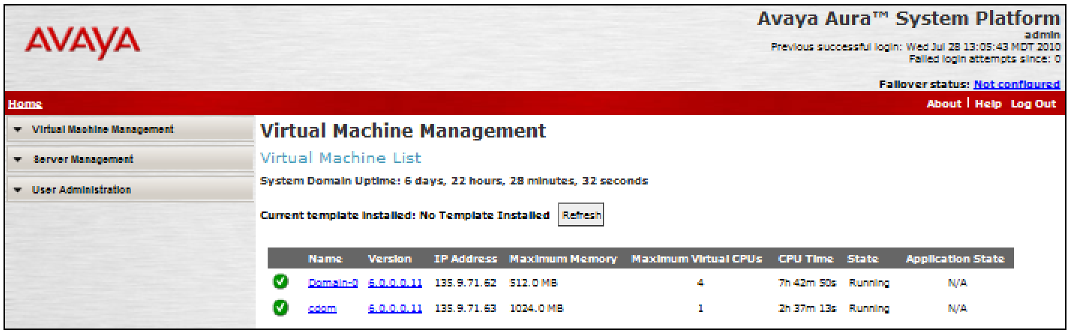
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.


AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
    - To change the schedule backup:
        i. Click **Change**.
        ii. On the Change Current Schedule Web page, click **Change Schedule**
    - To remove the schedule backup, click **Remove**.

      The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
    - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
    - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:

   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Upgrading the S8800 server to S8800 server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager configured as survivable remote (formerly known as LSP) from release 5.2.1 to release 6.0.1 using System Platform and the simplex survivable remote template on S8800 server.

In this procedure, you are required to upgrade an S8800 running Communication Manager 5.2.1 and reuse the same server to run System Platform and the simplex survivable remote template (CM_SurvRemote).

The simplex survivable remote template supports:

- Communication Manager
- Utility server

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager release 6.0.1.

Perform the following additional tasks to reuse the existing server:

- Increase the memory
- Add a third hard drive
- Update the uEFI firmware
- Reconfigure the RAID controller to support RAID 5
- Update the uEFI settings

Note:

For instructions to update the uEFI firmware and uEFI settings, download the release notes from the Avaya Support Web site at http://support.avaya.com.

For more information see, the *Avaya S8800 Migration Kit*.

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade.

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager template	
	Verify that you have all the necessary equipment onsite, for example: • Hard disk drive • Memory module • Services laptop and crossover cable • Electrostatic wrist ground strap and mat	For the list of required equipment, see *Avaya Migration Kit.*
	Obtain the CD to update the uEFI firmware using one of the following ways: • Order the uEFI firmware CD • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.	
	Obtain the RIAD 5 firmware CD	

✔	Task	Description
	Obtain the CD to update the uEFI settings using one of the following ways: • Order the uEFI settings CD • Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Documentation checklist for server upgrades

You need the following additional documentation:

✔	Task	Description
	Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603444.	Provides instructions for installing the S8800 Server for Communication Manager.
	Installing and Configuring Avaya Aura™ Communication Manager, 03-603558.	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.

2. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.
       The configuration screen appears in your application window.
    b. Click **File** and select **Save As**.
    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**

- **Set Identities**
- **Configure Interfaces**
- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging in from a laptop directly connected to the services port, perform one of the following:
    - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
    - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, Select **Full Backup** (release-dependent).

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Verifying the hardware on the server

Verify the memory, hard drive, and RAID configuration on the existing server:

1. Log on to System Management Interface and select **Administration** > **Server (Maintenance)**.
2. Under **Server Configuration**, select **Display Configuration**.
3. Under **Disk devices**, verify if the system has three 146GB hard disk drives. If the system does not have three disk drives, install a disk drive on the server later when you are instructed to do so.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

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

```
Backup successful
```

Caution:

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the cables

1. Label and disconnect the power cord(s) from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server cover

Prerequisites

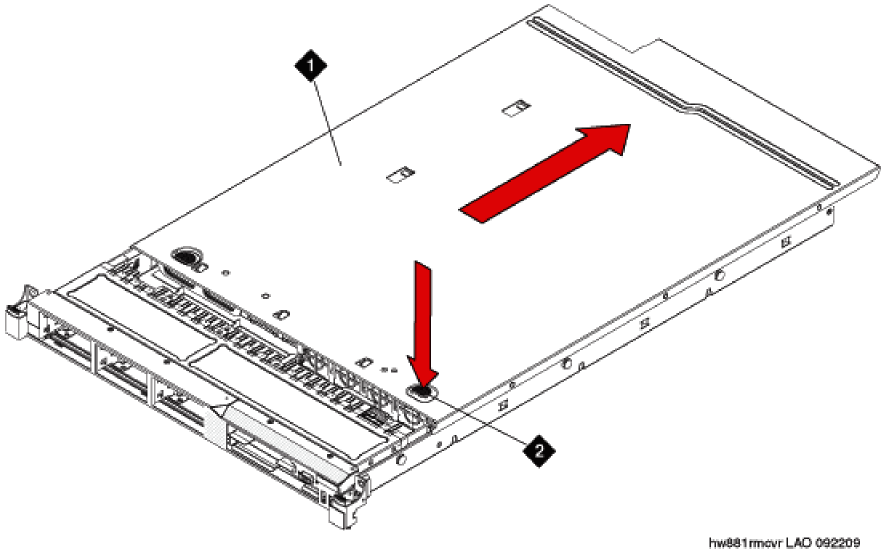
Before you disconnect the server from the power source, make a note of which LEDs are lit, including the LEDs that are lit on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs are not lit when the power source is removed.

Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

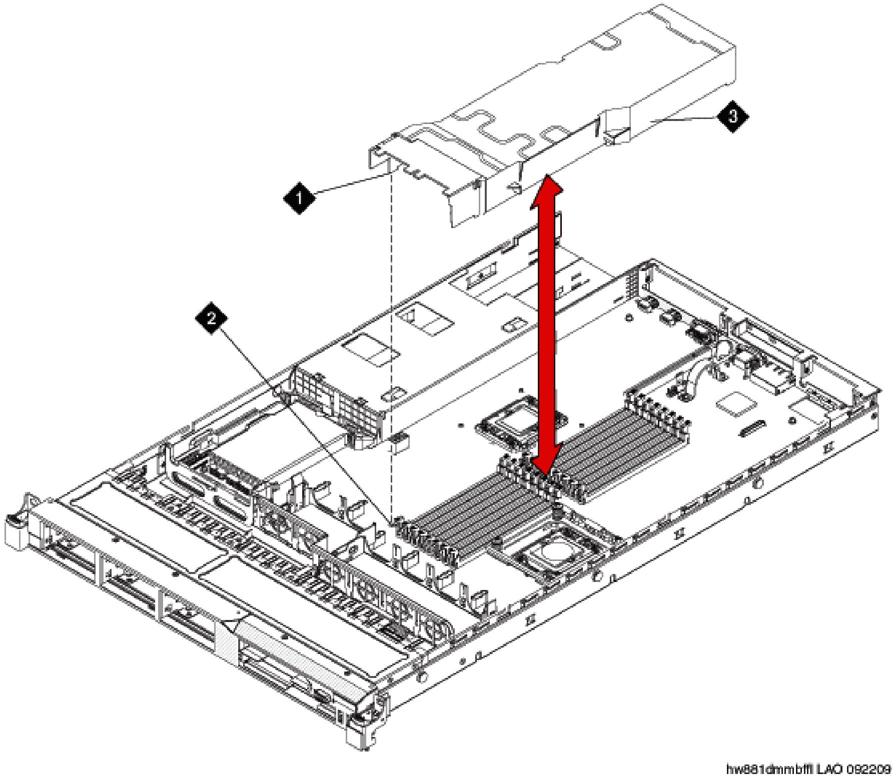
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Grasp the DIMM air baffle and lift the air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Prerequisites

Remove the DIMM air baffle.

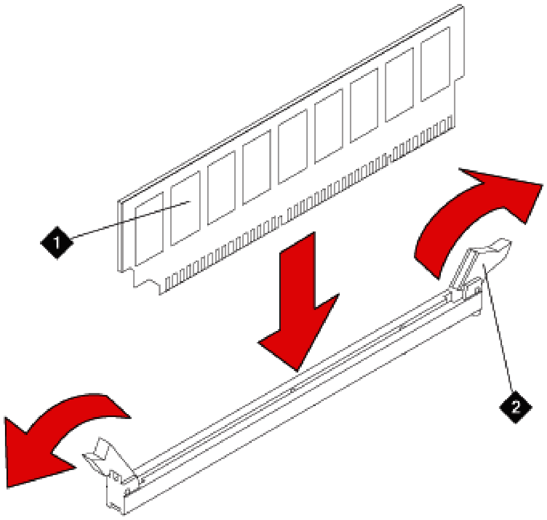
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.
   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

Important:

If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.

7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.
    When you install or remove memory modules, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

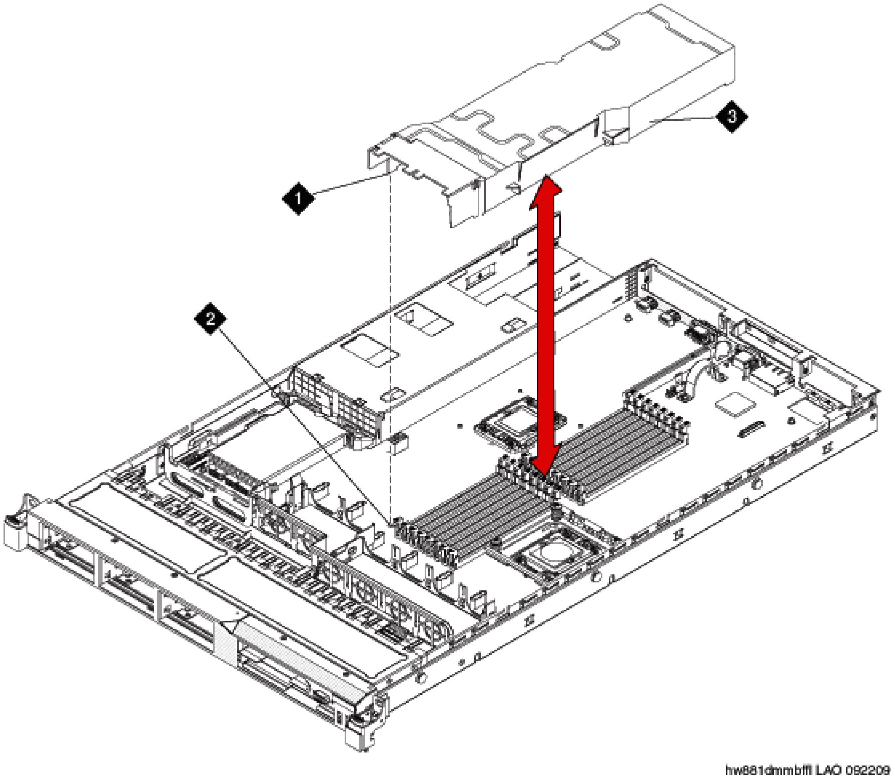
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

Prerequisites

If replacing an existing hard drive, remove the hard drive that you want to replace.

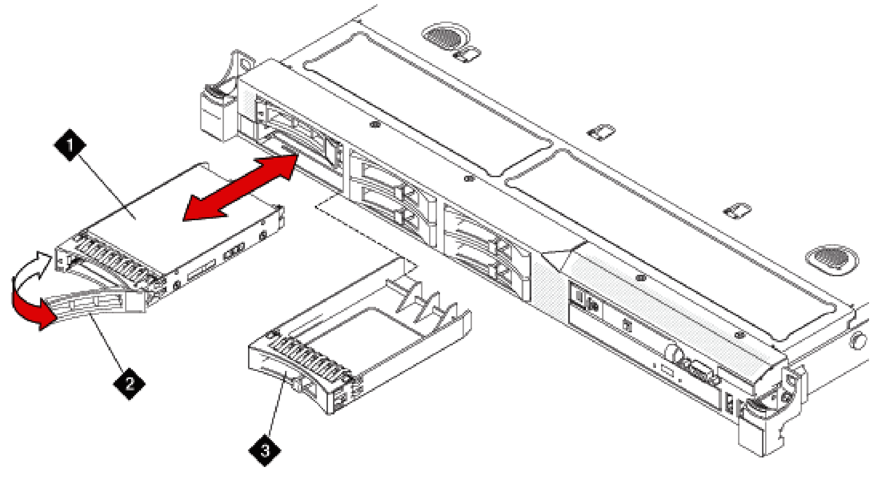
Important:

To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



hw881inhdd LAO 092309

1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. If the amber LED remains lit, the drive is faulty and must be replaced.

Updating S8800 server firmware

Prerequisites

- Obtain the CD for uEFI firmware. You must either order the CD or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Prerequisites

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.
2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration &
   Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server,

reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Next steps

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

Prerequisites

- Obtain the CD for uEFI settings of S8800 Server. You may order the CD, or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

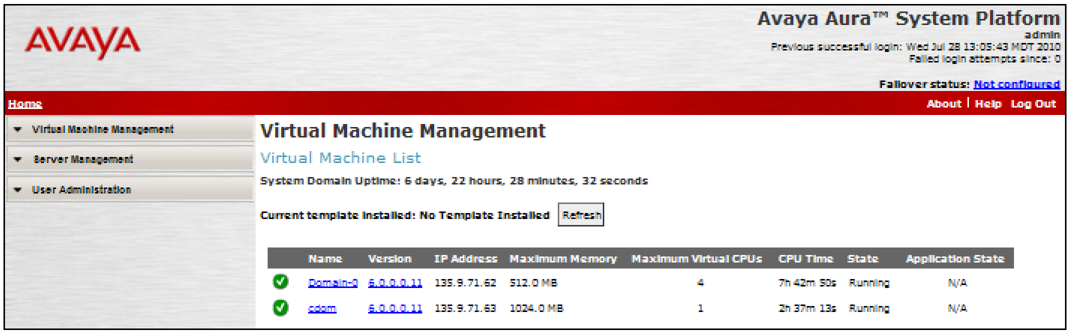
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Fallover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.

3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Upgrading DEFINITY SI or R Server to the S8800 Server

Introduction

This section describes the procedure to upgrade the following servers to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server or Dell™ PowerEdge™ R610 Server:

- DEFINITY SI Server in an SCC1 or an MCC1
- DEFINITY R Server in an MCC1

In this procedure:

- You discard:
    - All port networks (SCCs or MCCs)
    - SI or R processor circuit pack
- You install:
    - A G650 Media Gateway and move the supported circuit packs to the media gateway.
    - An S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex survivable remote template (CM_SurvRemote).

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

This upgrade affects service. When you turn off the PPN stack to replace the cabinet as part of the upgrade process, the system drops all calls. Service returns when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following server, as appropriate: - S8800 Server	

✔	Task	Description
	- Dell™ PowerEdge™ R610 Server - HP ProLiant DL360 G7 Server • G650 Media Gateway • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP or later C-LAN	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	Installing the Avaya G650 Media Gateway (03-300685)	Provides instructions for installing and configuring the G650 Media Gateway.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PNs to prepare the DEFINITY system for upgrade. The changing or upgrading the hardware includes:

- Changing TN2182 Tone Clock and maintenance circuit packs for TN2312BP IP Server Interfaces (IPSI) and new TN779D maintenance circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service. However, duplex-reliability configurations encounter short service interruptions when you change the tone-clock circuit pack is in IPSI-controlled PNs.

Server and IPSI cable connections

Each IPSI circuit pack must have a CAT5 cable that connects to the customer network. Cables for IPSIs are located in PN carrier A. If the system has a duplicated bearer network, the cables for IPSIs are located in PN carrier B.

In duplex configurations, each server is connected to the customer network that comprise control network A (CNA). If this system has duplicated IPSIs, each server is connected to the customer network that comprise control network B (CNB).

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Replacement of circuit packs

All PNs receive IPSI circuit packs. The TN2312BP IPSI circuit pack replaces the existing TN2182 Tone Clock circuit pack and terminates control communication with the servers. Flat ribbon cables run between the IPSIs and the maintenance circuit pack. These ribbon cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit packs, program static IP addresses into the IPSIs.

You can complete this stage at any time before the cutover. The tone clock and the IPSI circuit packs are hot swappable, and you replace the circuit packs in the existing DEFINITY system without the need to turn off the power.

The IPSI circuit pack provides the same functionality as the tone clock circuit pack. You perform the following tasks before the cutover:

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSIs are working as tone clocks in the existing system.
- Test the connectivity between the server and the IPSI.
- Reinstall the IPSIs in the new carriers after you install the carriers.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Prerequisites

A cross-over cable to connect your services laptop directly to the processor.

1. Perform one of the following tasks to connect the services laptop to the processor:
    - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
    - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

    This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).
- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura ™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled

for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

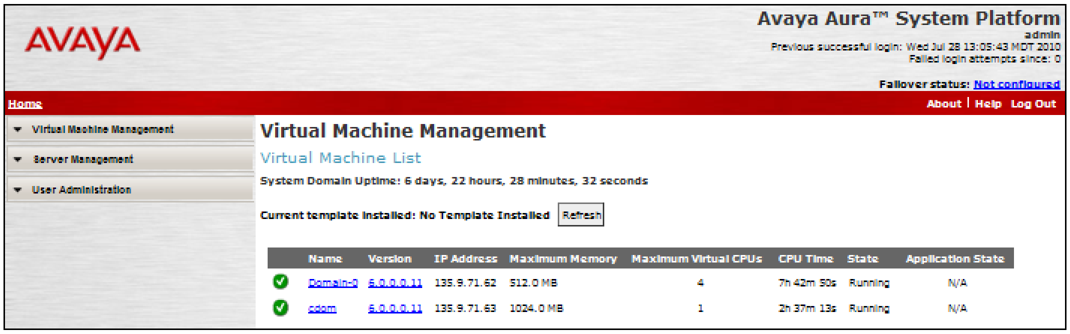
Note:

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

   For more information, see About subnet address.

3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing G650 Media Gateway in the rack

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.
6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.

   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.

7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
    a. Enter `exit`.

       The system saves the changes and ends the IPSI session.

    b. Enter `192.11.13.6` and log in to the IPSI.
    c. Enter `show control interface`.

       The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

    d. Enter `reset` and press `Enter`.

       Add or copy the login portion before you add the control gateway.
9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.
4. For G650, if the maintenance function is used:
   a. Connect one end of the serial maintenance cable to the DB9 connector on the IPSI adapter.
   b. Connect the other end to the Emergency Transfer panel to provide 1 alarm output and 2 alarm inputs.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
    - TN2312BP IPSI
    - TN799DP Control-LAN (C-LAN)
    - TN2302AP or TN2602AP IP Media Processor

    If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Port network circuit packs

Because you do not reuse the PPN after the upgrade, you must:

- Relocate the port network circuit packs to a new G650 Media Gateway.
- Remove all port network circuit pack translations related to the PPN. The STS group manages the translation changes necessary for this upgrade.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.

5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you might also need to adjust the administration of the network regions. Your planning documents might provide information about changes to network regions. For more information on how to administer network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit packs

Prerequisites

Start a SAT session.

Complete Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6

- DiffServ: 46

3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface UUCSS` to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

The default is **none**.

Removing fiber-related administration

Prerequisites

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Administering PN synchronization

Prerequisites

Open a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
    - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
    - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network` *n*, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

The system displays a list of all the cabinets and the PNs that the cabinets contain under **Circuit Packs Available for Synchronization**.

5. Obtain a location for the synchronization source circuit pack from the list under **Circuit Packs Available for Synchronization** for **Primary** and **Secondary** fields. Ensure that you choose a working synchronization source.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, add another synchronization-source circuit pack location in the **Secondary** field.
8. Press **Submit**.

   Wait about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization-switch all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must show `PASS` in the **Results** field. If the **Results** field does not show `PASS`, you must troubleshoot the synchronization error.

Completion tasks on the cabinet

Disconnecting from the server

Unplug the laptop from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

1. Remove the fiber cables that connect the following circuit packs in the PNs:

   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B

2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Cutover to the server control

Because you do not reuse the PPN, you relocate the port network circuit packs to G650 Media Gateway.

When you relocate the circuit packs to the media gateway and you turn on the power, you want to cut over to have the new server control the existing PNs. The server can be an S8800 Server, Dell™ PowerEdge™ R610 Server or an HP ProLiant DL360 G7 Server. To cut over to the server, you must enable the IPSIs on the IP Server Interface (IPSI) System Parameters screen.

This stage affects service momentarily while the CSS comes up and the calls are load balanced across the IPSIs throughout the port networks.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   ⚠ **Caution:**

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

   Note:

   You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or the customer wants to minimize out-of-service time.
4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on the new server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.

2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
    - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
    - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:

   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Chapter 5: Upgrading to duplex main/survivable core template

Upgrading the S8500A Server to S8800 Server

Introduction

Use this procedure to upgrade S8500A simplex server running Communication Manager releases 2.0 through 3.x to Release 6.0.1 on S8800 Servers. The complete list of releases in this range is available at www.support.avaya.com.

Note:

Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.

In this procedure, you replace the S8500A server by a pair of S8800 Servers running System Platform and the duplex main/survivable core template.

The upgrade procedure involves:

- Creating a data set with specific information of the existing simplex server that you later restore on Communication Manager Release 4.0.5.
- Installing Communication Manager Release 4.0.5 on the first S8800 server and restoring the backed up data from the existing server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5.
- Creating a data set with specific information that you later restore on both Communication Manager Release 6.0.1 servers.
- Installing System Platform and Communication Manager duplex main/survivable core template on both S8800 servers.
- Restoring the data set that was created while on Release 4.0.5.

Note:
You must restore the upgrade dataset backed up from the staged S8800 simplex server to both S8800 servers.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Use this section to upgrade Communication Manager from releases 2.0 through 3.x to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager - CD-ROM for Communication Manager Release 5.2.1 - DVD for Communication Manager Release 6.0.1 template	

Documentation checklist for server upgrades

You need the following additional documentation:

✔	Task	Description
	Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager, 03-603444.	Provides instructions for installing the S8800 Server for Communication Manager.
	Installing and Configuring Avaya Aura™ Communication Manager, 03-603558.	Provides instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:

- If onsite, connect to the services port labeled as *2* on the back of the media server.
- If offsite, log on to the media server using the unique IP address of the media server.

2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:

a. Right-click and select **Paste**.

   The configuration screen appears in your application window.

b. Click **File** and select **Save As**.

c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Print or copy the information from the following screens:

   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**

7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.

8. Click **Administration** > **Server (Maintenance)**.

9. Print or copy the information from the following screens:

   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.

11. On the command line prompt, perform the following:

    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

    c. Enter `almsnmpconf` and record the output.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**

Starting a SAT session

Prerequisites

If you are using Telnet, enable the Telnet service for Communication Manager.

If Telnet is disabled, use SSH to access the SAT.

Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.

- If you are logging on to the server with a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
    - Select **Full Backup**.
    - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
        1. Select **Specify Data Sets**.
        2. Select the check boxes:
            - **Avaya Call Processing (ACP) Translations**
            - **Server and System Files**
            - **Security Files**
3. In the **Download size** field, enter the size of the backup `.tar` file.

    There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp]` or `[all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Preupgrade service packs

You do not need the following preupgrade patches to upgrade S8500A Server running Communication Manager release 2.x to Release 4.0.5 on S8800 server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Service pack for the current software version

You must obtain and activate the latest available service pack for the currently running Communication Manager software version before you proceed with the next upgrade steps. Depending on the release, use one of the following procedures to install the service pack.

Installing service pack updates

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. Enter `cd /var/home/ftp` to access the `ftp` directory.
5. At the prompt, enter `ls -ltr` to list the files in the `ftp` directory.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`.

   Here, *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes. However, wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show` to list the files to verify that the new software file is installed.

11. Enter `statapp -c` to view the status of the processes.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process has not come up and should be investigated before you proceed with the next upgrade step.

12. Close the Telnet session.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:

You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     2. Click **Yes**.
3. Click **Continue**.

Note:
Do not install the preupgrade service pack until instructed.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

  If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up files to localhost

Prerequisites

Enable FTP service.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, select **Network Device** and complete the following fields:
   - In the **Method** field, select `FTP`.
   - In the **User Name** field, enter `anonymous`.
   - In the **Password** field, enter `2` or `@`.
   - In the **Host Name** field, enter `localhost`.
   - In the **Directory** field, enter `/pub`.

4. Click **Start Backup**.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.
   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```
   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

The system closes the ftp session.

8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Note:
Do not shutdown the server at this time.

The S8500A server continues to provide service until later in the procedure. Do not shut down the S8500A server until instructed.

Upgrade tasks on the S8800 (Release 5.2.1) Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).

- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

- HP ProLiant DL360 G7 Server

For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing Communication Manager Release 5.2.1

Prerequisites

- Install the new server in the rack.
- Insert the CD-ROM for Communication Manager Release 5.2.1 into the drive of the server.
- Turn on the server.

1. On your laptop, click **Start** > **Run**.
2. In the Run dialog box, enter `telnet 192.11.13.6` and press `Enter`.

   To navigate on the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install**, highlight **OK** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.
5. When the system prompts you, select SIMPLEX.
6. Select CM only.

   Do not select CM with CMM or CMM stand-alone options.

   The installation process:

   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.

   The installation process takes about 20 minutes. When the server is ready to reboot, the CD/DVD drive door opens and a reminder to check the Avaya Support Site at http://support.avaya.com for the latest software and firmware updates appears on the screen. Remove the CD from the drive.

   The reboot takes about 5–8 minutes. The Telnet session ends automatically.

Checking the reboot progress

1. On the laptop, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
    - The system displays the command line prompt if the cache is cleared.
    - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

    The -t causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Verifying the software version

1. At a browser on your services laptop log on to the System Management Interface (192.11.13.6).
2. Select **Administration > Server (Maintenance) > Software Version**.
    The system displays the Software Version page.
3. Verify that the server is running Release 5.2.1 software. The beginning of the CM Reports as: string should show `R015x.02.1.xxx.x`
4. Verify that the optical drive opened at the end of the software installation.

Setting date, time, and time zone

1. Click **Administration** > **Server (Maintenance)**.
2. Under **Server**, click **Server Date/Time**.
3. Change the date, time, and time zone as needed.
4. Click **Submit**.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Using the steps described in this section, you can download the following files:

- The latest available service pack for Communication Manager Release 4.0.5 or Release 5.2.1
- The RFA license for Communication Manager Release 4.0.5 or Release 5.2.1
- Avaya authentication file for Communication Manager Release 4.0.5 or Release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager Release 4.0.5 or Release 5.2.1
- One of the following backup sets:
    - The three-part backup, `os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`
    - Full backup, `full_*.tar.gz`

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     ii. Click **Yes**.
3. Click **Continue**.

   Note:
   Do not install the preupgrade service pack until instructed.

Creating a super-user login

Note:
The craft level login can create a super-user login.

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

   Note:
   Ensure that the customer can change this login, its password, or its permissions.
2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**
   The system displays the Administrator Accounts page.
3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.
   The system displays the Administrator Logins -- Add Login: Privileged Administrator page.
5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

   Note:
   Do not lock the account or set the password to be disabled.
9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.

10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.
    The system informs you the login is added successfully.

Installing the Communication Manager license and authentication files

⚠ **Caution:**

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 111.

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.
   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.
   The system displays a message indicating that the license is installed successfully.
3. Click **Restart CM**.
4. Under **Server**, click **Process Status**.
5. Under **Frequency**, select Display Once.
6. Click **View**.
7. Verify that all operations are `UP`.
8. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.
   The system displays the Authentication File page.
9. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.
   The system displays a message indicating that the authentication file is installed successfully.

Restoring server data

Prerequisites

- Ensure that the license file is valid.

  Note:
  You do not need a license file for survivable core server and survivable remote server.

- Copy the datasets to the server.
- Install the latest service pack for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Depending on the release of Communication Manager of the existing system, the data you restore comes from:

- The three-part backup (os, security, xln) or a full backup
- The backup files copied to the flashcard or the laptop

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - If the backup file is copied to the laptop, click **Local Directory**.

     The fields displays the default directory `/var/home/ftp/pub`. Keep the default directory.
   - If the backup file is copied to the flashcard, click **Local CompactFlash Card**.
3. Click **View**.
4. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
5. Select both **Force** options.
6. Click **Restore**.
7. To view the status of the restore process:
   1. Click **Restore History** and select the file you want to restore.
   2. Click **Status**.
      When the restoration is complete, the system displays the message `backup: 0: restore of <filepath/filename> completed successfully.`

Result

You may lose connectivity between the laptop and the server. Ignore this condition and proceed to the next steps.

Rebooting the server

Use this procedure to reboot the server if the connectivity between the laptop and the server is lost after you restore the data.

Note:

If the connectivity between the laptop and the server is available after you restore the data, use **Server** > **Shutdown Server** on System Management Interface to reboot the server.

1. Press the power control button for several seconds on the front of the server.
   The server turns off.
2. Press the power control button again.
   The server turns on.

Connecting the services laptop to the server

Prerequisites

- Wait for about 5–8 minutes for the system to complete the reboot.
- Verify if ping from the laptop to server is successful.

If the connectivity, ping test, between the laptop and the server is functional, proceed with the section “Accessing the System Management Interface”.

Complete this procedure only if the laptop connected to the services port, the port labeled **2**, is not functional after the reboot.

1. Disconnect the laptop from the Ethernet port labeled **2**.
2. Connect the laptop to the Ethernet port labeled **4**.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.

   ii. The system displays the status as the update progresses. The system automatically reboots, if required.

   iii. Click **Yes**.

3. Click **Continue**.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up files to localhost

Prerequisites

Enable FTP service.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, select **Network Device** and complete the following fields:
   - In the **Method** field, select `FTP`.
   - In the **User Name** field, enter `anonymous`.

- In the **Password** field, enter `2` or `@`.
- In the **Host Name** field, enter `localhost`.
- In the **Directory** field, enter `/pub`.

4. Click **Start Backup**.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message: `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.
   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget migration-60*
     y
     quit
     ```
   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     ```

```
get <name of the backup file>
quit
```

For example, `migration-60_cmserver_172731_20100516.tar.gz`.

The system closes the ftp session.

8. To confirm that the backup file, for example, `migration-60*.tar.gz` is present, enter `dir migration*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

The S8500A server continues to provide service until later in the procedure. Do not shut down the S8500A server until instructed.

Upgrade tasks on the S8800 (Release 6.0.1) Server

Turning on the server

Prerequisites

Do not connect the server to the network.

1. Insert the System Platform DVD into the CD/DVD drive of the server.
2. Turn on the server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled

for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

    Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

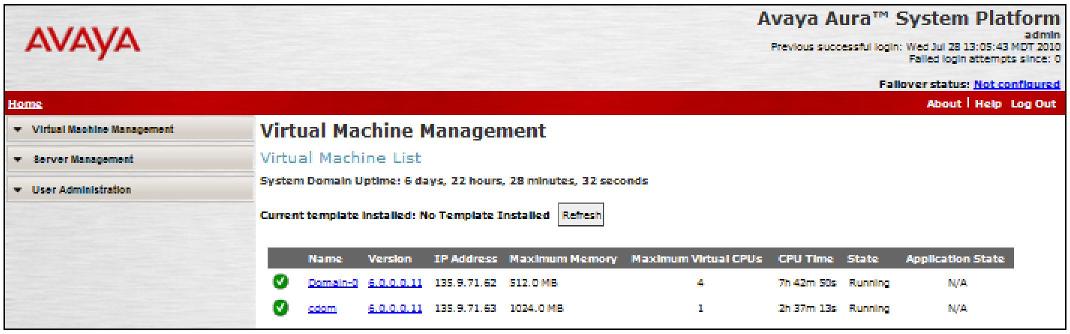
Note:

This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:

You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

Use this procedure to copy the service packs or the upgrade data set (for example, migration-60*.tar.gz file) to the server.

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Note:

You must restore the upgrade dataset backed up from the staged S8800 simplex server to both S8800 servers.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:
You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

      Important:
      If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Completion tasks on the active S8500A Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Important:
Service outage begins at this point of the upgrade process.

Postupgrade tasks on the first S8800 (Release 6.0.1) active server

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays:
    - `UP` for all operations
    - `Down` for `dupmgr`
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Perform this procedure on the main server only.

Enter `save translation all`.
The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:
   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Postupgrade tasks on the second S8800 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).
- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the server

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

     Important:
     Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:
You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

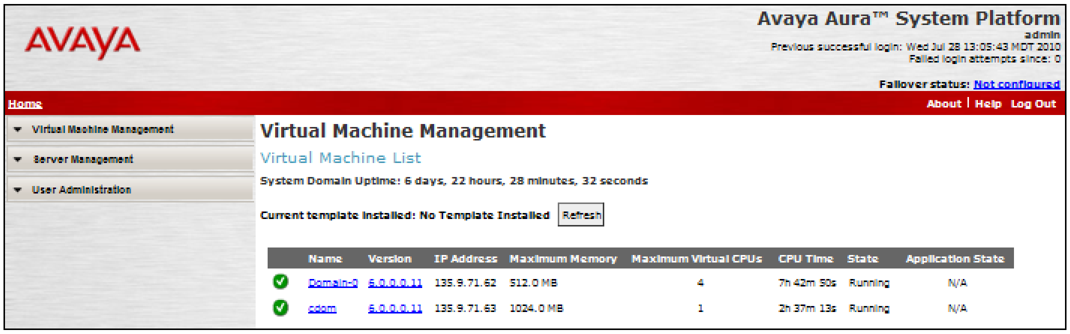
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.
   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Note:

You must restore the upgrade dataset backed up from the staged S8800 simplex server to both S8800 servers.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the connection for server duplication

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, click **Other server via duplication link**.
3. Click **Execute Ping**.
   If the two endpoints are connected, the system displays, `MessRecv`: `1`.
4. Under **Server**, click **Status Summary**.
   a. Verify that this server is in `BUSY OUT` mode.
   b. Verify that the other server is in `Active` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link`: `up`.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay

3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.
   The roles of the active and standby servers changes.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500B or S8500C Server to S8800 Servers

Introduction

Use this procedure to upgrade S8500B or S8500C simplex server running Communication Manager Release 4.0.5 or Release 5.2.1 to S8800 Servers,Dell™ PowerEdge™ R610 Servers or HP ProLiant DL360 G7 Servers running Release 6.0.1.

In this upgrade procedure, you replace the S8500B or S8500C simplex server with S8800 servers running System Platform and the duplex main/survivable core template.

Duplex main/survivable core template on Communication Manager Release 6.0.1 and later does not support Communication Manager Messaging.

Important:

If the S8500B or S8500C Server has Communication Manager Messaging installed on it, after the upgrade, messaging will not be available on the system. To have messaging on your upgraded system, Avaya recommends that you purchase Avaya Aura® Messaging.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8500B or S8500C server to Communication Manager Release 4.0.5 or Release 5.2.1. For instructions, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.0.1.
3. Perform the upgrade to Release 6.0.1 as described in this section.

Note:
You restore the upgrade dataset backed up from the S8500B or S8500C Server to both S8800 Servers.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information on how to accomplish this task, and about specific commands, see:

- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431)
- *Avaya Aura™ Communication Manager Server Alarms* (03-602798)

Prepgrade tasks on the S8500B or S8500C server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**

- **Set Identities**
- **Configure Interfaces**
- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Verifying the current software release

1. Under **Server**, click **Software Version**.
   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, Select **Full Backup** (release-dependent).

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.

3. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large.

4. Under **Backup Method**, select **Network Device** and select a method from the provided options.

5. Fill in the following fields:

   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**

6. Click **Start Backup**.

7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**

- **Password**
- **Host Name**
- **Directory**

The backup location must be a server on the customer LAN.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

5. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Installing both S8800 servers in the rack

Install the S8800 servers in the rack. For more information, see *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603444).

At this point do not connect the servers to any network.

Duplex main/survivable core template

You are required to install duplex main/survivable core template on each server using a new host name and new IP address.

After you complete the duplex main/survivable core template installation and restore the upgrade dataset, you must configure each server in the server pair to use the Communication Manager Release 5.2.1 server host name and IP address for the Communication Manager Release 6.0.x server configuration for **Alias Host Name** and **Alias IP address**. Refer Communication Manager upgrade simplex to duplex template - worksheet on page 1359 for the worksheet to use for configuring the server.

Upgrade tasks on the first S8800 Server

The S8500B or S8500C server continues to provide service until later in the procedure. Do not shut down the S8500B or S8500C server until instructed.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:
If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the new server

1. Do not connect the server to the network until you are instructed to do so.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

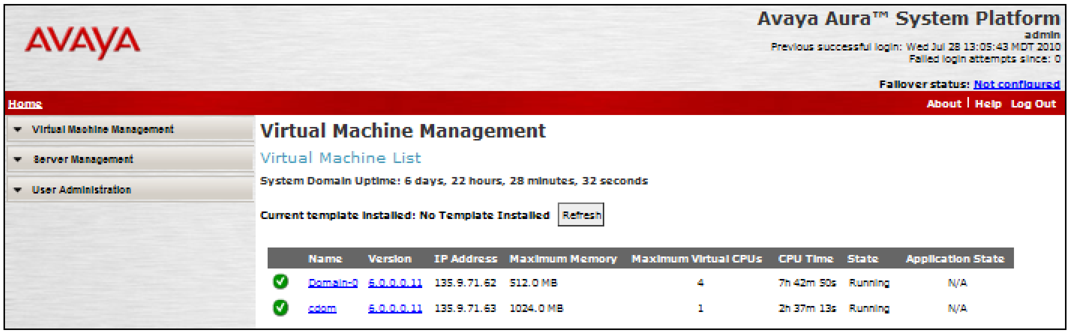
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.

3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Note:

You must restore the upgrade dataset backed up from the staged S8800 simplex server to both S8800 servers.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.

2. On the View/Restore page, perform one of the following:

   - Click **Network Device** and complete the following fields:

     - **Method**

     - **User Name**

        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    > **Important:**
    > If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Completion tasks on the active S8500 Server

Shutdown the active S8500 Server as outlined in the following procedure and connect the first S8800 Server to the network.

Important:

After you shutdown the active S8500 Server, at this point, the service will be down. To minimize the downtime, shut down the active S8500 Server, access the first S8800 Server again and release the server in the shortest amount of time possible.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Removing the server from the rack

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

On the first S8800 Server

Accessing the S8800 server

1. Clear the ARP cache on the laptop, if necessary.
2. Open a Web browser and connect to the server.
3. Log on to the server using System Management Interface.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Reset the settings that you recorded Disabling scheduled maintenance on page 37.

Saving translations

Perform this procedure on the main server only.

Enter `save translation all`.
The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.

3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Upgrade tasks on the second S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

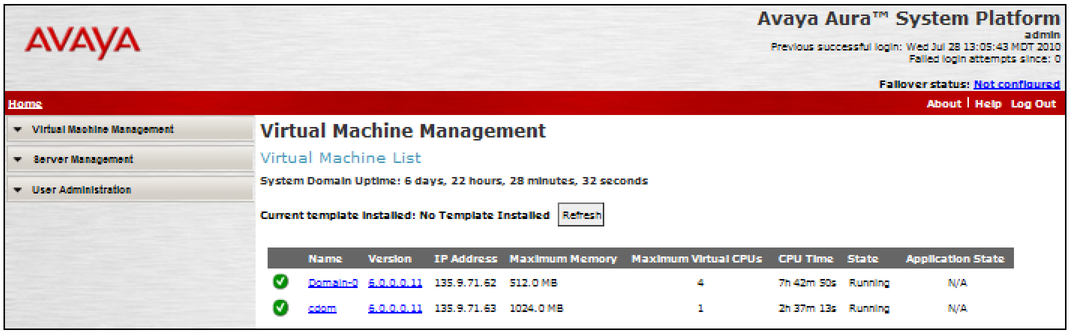
   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.

4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Connecting the cables to the server

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

   Important:
   Do not release the server until instructed.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you

plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**

    - **Host Name**
    - **Directory** or **Field Path**
        - If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
        - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:
If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
    - To change the schedule backup:
        i. Click **Change**.
        ii. On the Change Current Schedule Web page, click **Change Schedule**
    - To remove the schedule backup, click **Remove**.

      The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:
   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.

The roles of the active and standby servers changes.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8510 server to S8800 servers

Introduction

Use this procedure to upgrade S8510 simplex server running Communication Manager Release 5.2.1 to S8800 Servers running Release 6.0.1.

In this upgrade procedure, you replace the S8510 simplex server with S8800 Servers running System Platform and the duplex main/survivable core template.

Note:

Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.

Duplex main/survivable core template on Communication Manager Release 6.0.1 and later does not support Communication Manager Messaging.

Important:

If the S8510 Server has Communication Manager Messaging installed on it, after the upgrade, messaging will not be available on the system. To have messaging on your upgraded system, Avaya recommends that you purchase Avaya Aura® Messaging.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8510 Server to Communication Manager Release 5.2.1. For instructions, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.0.1.
3. Perform the upgrade to Release 6.0.1 as described in this section.

Note:

You restore the upgrade dataset backed up from the S8510 Server to both S8800 Servers.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information on how to accomplish this task, and about specific commands, see:

- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431)
- *Avaya Aura™ Communication Manager Server Alarms* (03-602798)

On the S8510 server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

      If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
    - LAN access by host name

      If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
    - Portable computer access by IP address

      If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.
    The configuration screen appears in your application window.
    b. Click **File** and select **Save As**.
    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
    d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**
    - **Set Identities**
    - **Configure Interfaces**
    - **Set DNS/DHCP**
    - **Set Static Routes**
    - **Configure Time Server**
    - **Server Access**
    - **Server Date/Time**
    - **Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for product ID.

Verifying the current software release

1. Under **Server**, click **Software Version**.
   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
    - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

      This means that Communication Manager Release 4.0.5 is running on the server.
    - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, Select **Full Backup** (release-dependent).

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.

3. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large.

4. Under **Backup Method**, select **Network Device** and select a method from the provided options.

5. Fill in the following fields:

   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**

6. Click **Start Backup**.

7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**

- **Password**
- **Host Name**
- **Directory**

The backup location must be a server on the customer LAN.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Installing both S8800 servers in the rack

Install the S8800 servers in the rack. For more information, see *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603444).

At this point do not connect the servers to any network.

Duplex main/survivable core template

You are required to install duplex main/survivable core template on each server using a new host name and new IP address.

After you complete the duplex main/survivable core template installation and restore the upgrade dataset, you must configure each server in the server pair to use the Communication Manager Release 5.2.1 server host name and IP address for the Communication Manager Release 6.0.x server configuration for **Alias Host Name** and **Alias IP address**. Refer Communication Manager upgrade simplex to duplex template - worksheet on page 1359 for the worksheet to use for configuring the server.

Upgrade tasks on the first S8800 Server

The S8510 server continues to provide service until later in the procedure. Do not shut down the S8510 server until instructed.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:

If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the new server

1. Do not connect the server to the network until you are instructed to do so.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

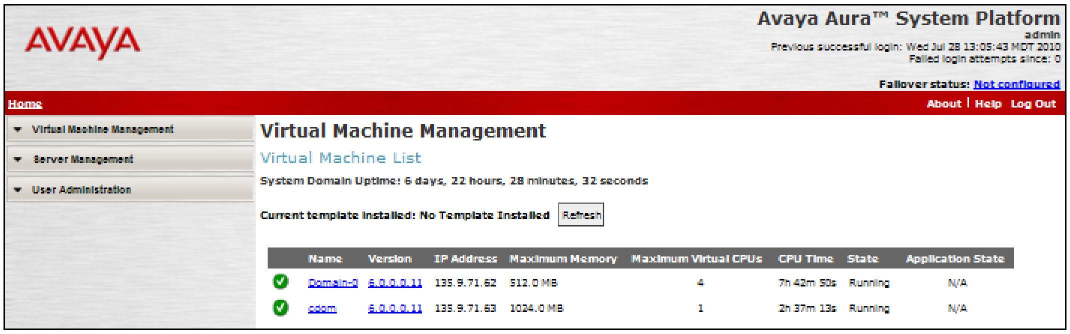
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Fallover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Note:

You must restore the upgrade dataset backed up from the staged S8800 simplex server to both S8800 servers.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Completion tasks on the S8510 Server

You need to perform the following two procedures on the S8510 Server.

> **Important:**
> After you complete these two tasks, at this point, the service will be down as the S8510 Server is shutdown. To minimize the downtime, shut down the S8510 Server, access the first S8800 Server again and release the server immediately.

You must continue to perform upgrade procedures on first S8800 Server.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Removing the server from the rack

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Postupgrade tasks on the first S8800 Server

Accessing the S8800 server

1. Clear the ARP cache on the laptop, if necessary.
2. Open a Web browser and connect to the server.
3. Log on to the server using System Management Interface.

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays:
    - `UP` for all operations
    - `Down` for `dupmgr`
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Reset the settings that you recorded Disabling scheduled maintenance on page 37.

Saving translations

Perform this procedure on the main server only.

Enter `save translation all`.
The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.

3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Upgrade tasks on the second S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   1. Start an SSH session.
   2. Log in to System Domain (Domain-0) as admin.
   3. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   1. Start an SSH session.
   2. Log in to System Domain (Domain-0) as admin.
   3. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

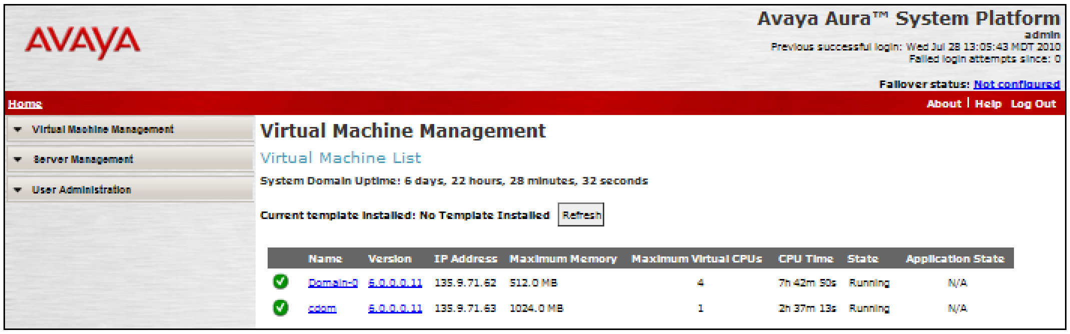
   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.

4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Connecting the cables to the server

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

   Important:
   Do not release the server until instructed.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you

plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**

  - Host Name
  - **Directory** or **Field Path**
    - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
    - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     i. Click **Change**.
     ii. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.

The roles of the active and standby servers changes.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8700-Series Servers to the S8800 Servers

Introduction

This section describes the two-step procedure to upgrade Communication Manager from:

1. Release 1.3.x, 2.x, 3.x or 4.x on S8700–Series Servers, which are not connected to the network, to Release 4.0.5 on S8800 Servers.
2. Release 5.x on S8700–Series Servers, which are not connected to the network, to Release 5.2.1 on S8800 Servers.
3. Release 4.0.5 or Release 5.2.1 on S8800 Servers to Release 6.0.1 on S8800 Servers, which will be connected to the network only later during this upgrade step.

In this upgrade procedure, you replace the S8700–Series Servers with S8800 Servers running System Platform and the duplex main/survivable template.

Note:

Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Overview on page 1375.

- For Communication Manager release 3.0 and later, perform the conversion before you upgrade the servers.
- For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

If you can upgrade the existing S8700-series Server to Communication Manager Release 4.0.5 or Release 5.2.1 without replacing the hardware, use the procedures outlined in *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885, Issue 1, May 2009).

If you cannot upgrade the existing S8700-series Server to Communication Manager Release 4.0.5 or Release 5.2.1 without replacing the hardware, use the two-step procedures outlined in this section.

Use the following procedures for each S8700-Series Server to upgrade to Release 5.2.1:

Server	Upgrade procedures	Comments
S8700	Use the procedures from the current section	Communication Manager Release 5.2.1 does not support S8700 Server.
S8710 with DAL1	Use the procedures from the current section	Would require DAL2 otherwise
S8710 with DAL2	Use the procedures from *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885)	
S8720	Use the procedures from *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885)	
S8730	Use the procedures from *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885)	

The upgrade procedure involves:

- Creating a data set with specific information of the existing servers that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Installing Communication Manager Release 4.0.5 or Release 5.2.1 on both S8800 Servers and restoring the backed up data from the existing server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.
- Installing System Platform and Communication Manager on both S8800 Servers.
- Restoring the data set that was created while on Release 4.0.5 or Release 5.2.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Preupgrade tasks on the active S8700 server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.
    The configuration screen appears in your application window.
    b. Click **File** and select **Save As**.
    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
    d. Click **Save**.
6. Print or copy the information from the following screens:
    - **Set Identities**
    - **Configure Interfaces**

- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**

7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
    b. Enter `productid` and copy the value for product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
    - **Telnet Server (23)**
    - **SAT (Telnet 5023)**

Starting a SAT session

Prerequisites

If you are using Telnet, enable the Telnet service for Communication Manager.

If Telnet is disabled, use SSH to access the SAT.

Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging on to the server with a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   > ⚠ **Caution:**
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - Select **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     1. Select **Specify Data Sets**.
     2. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**

3. In the **Download size** field, enter the size of the backup `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Converting fiber PNs to IP-PNC

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Overview on page 1375.

Note:

For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
    - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
    - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

    For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:
If this operation fails, follow the escalation procedures before you continue with the next step.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Preupgrade service packs

You do not need the following preupgrade patches to upgrade S8500A Server running Communication Manager release 2.x to Release 4.0.5 on S8800 server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Installing service pack updates

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. Enter `cd /var/home/ftp` to access the `ftp` directory.
5. At the prompt, enter `ls -ltr` to list the files in the `ftp` directory.

   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`.

   Here, *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and takes more than 2 minutes if messaging is enabled. However, wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. Enter `statapp -c` to view the status of the processes.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP or, if Communication Manager Messaging is installed, 67/67 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:
    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
    - If the status of the update file you want to activate is packed:
        1. Select the **update ID** and click **Unpack**.
        2. Wait until the system displays the message, `... unpacked successfully`.
    - If the status of the update file you want to activate is unpacked:
        1. Select the **update ID** and click **Activate**.

            The system displays the status as the update progresses. The system automatically reboots, if required.
        2. Click **Yes**.
3. Click **Continue**.

    Note:
    Do not install the preupgrade service pack until instructed.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

  If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up files to localhost

Prerequisites

Enable FTP service.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - For Communication Manager release 3.0 or later, select **Full Backup**.
3. Under **Backup Method**, select **Network Device** and complete the following fields:
   - In the **Method** field, select `FTP`.
   - In the **User Name** field, enter `anonymous`.
   - In the **Password** field, enter `2` or `@`.
   - In the **Host Name** field, enter `localhost`.
   - In the **Directory** field, enter `/pub`.
4. Click **Start Backup**.
5. Select the backup from the list and click **Check Status**.

When the backup is complete, the system displays the following message:
`Backup successful`

Caution:

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.
   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

The system closes the ftp session.

8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Note:
Do not shutdown the server at this time.

Preupgrade tasks on the standby S8700 Server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:
    - If onsite, connect to the services port labeled as *2* on the back of the media server.
    - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.

      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
   - **Server** > **Server Date/Time**
   - **Security** > **Server Access**
   - **Miscellaneous** > **CM Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:

a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

b. Enter `productid` and copy the value for product ID.

c. Enter `almsnmpconf` and record the output.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
    - **Telnet Server (23)**
    - **SAT (Telnet 5023)**

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - Select **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     1. Select **Specify Data Sets**.
     2. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
3. In the **Download size** field, enter the size of the backup `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:

- **User Name**
- **Password**
- **Host Name**, enter the host IP address.
- **Directory**

6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   > **Note:**
   >
   > ***Do not*** select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Preupgrade service packs

You do not need the following preupgrade patches to upgrade S8500A Server running Communication Manager release 2.x to Release 4.0.5 on S8800 server.

- 00.0.219.0-1205 (2.0)
- 00.1.221.1-1204 (2.0.1)
- 01.0.411.7-1203 (2.1)
- 01.1.414.1-1203 (2.1.1)
- 02.0.111.4-1204 (2.2)
- 02.1.118.1-1201 (2.2.1)
- 02.2.122.0-1201 (2.2.2)

Installing service pack updates

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack for the currently running Communication Manager release and activate it.

Use this procedure if the server is running Communication Manager release earlier than 4.0.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. Enter `cd /var/home/ftp` to access the `ftp` directory.
5. At the prompt, enter `ls -ltr` to list the files in the `ftp` directory.
   The system displays a list of files in the `ftp` directory.
6. Verify that the `ftp` directory contains the `*.tar.gz` file that you uploaded.
7. Enter `sudo patch_install patch.tar.gz`, where *patch* is the release or issue number of the service pack file, for example, `03.1.526.5-1003.tar.gz`.

8. Enter `patch_show` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch`.

   Here, *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and takes more than 2 minutes if messaging is enabled. However, wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show` to list the files to verify that the new software file is installed.
11. Enter `statapp -c` to view the status of the processes.

    Ensure that all operations except dupmgr shows `UP`. Communication Manager should show 65/65 UP or, if Communication Manager Messaging is installed, 67/67 UP. To stop the continual refresh of the **`statapp`** command, enter `Ctrl-C`.

    Note:
    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:

i. Select the **update ID** and click **Unpack**.

ii. Wait until the system displays the message, `... unpacked successfully`.

- If the status of the update file you want to activate is unpacked:

i. Select the **update ID** and click **Activate**.

The system displays the status as the update progresses. The system automatically reboots, if required.

ii. Click **Yes**.

3. Click **Continue**.

Note:
Do not install the preupgrade service pack until instructed.

Communication Manager backup

You must perform this backup for an upgrade to Release 4.0.5 or Release 5.2.1.

You can back up the translation files (xln), the system files (os), and the security files to:

- Flash card using the USB-connected external compact flash drive
- Localhost

If you choose to back up the files to localhost, you must enable the FTP service.

Backing up the files to flashcard

Prerequisites

Log on to the server using System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
     - **Avaya Call Processing (ACP) Translations**

  - **Server and System Files**
  - **Security Files**
- For Communication Manager release 3.0 or later, select **Full Backup**.

3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up files to localhost

Prerequisites

Enable FTP service.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:

- For Communication Manager releases earlier than 3.0, select **Specify Data Sets** and select the following check boxes:
    - **Avaya Call Processing (ACP) Translations**
    - **Server and System Files**
    - **Security Files**
- For Communication Manager release 3.0 or later, select **Full Backup**.

3. Under **Backup Method**, select **Network Device** and complete the following fields:
    - In the **Method** field, select `FTP`.
    - In the **User Name** field, enter `anonymous`.
    - In the **Password** field, enter `2` or `@`.
    - In the **Host Name** field, enter `localhost`.
    - In the **Directory** field, enter `/pub`.
4. Click **Start Backup**.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

Caution:

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.

For example, `technician@companyname.com`.

7. At the `ftp` prompt:

   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget full_*
     y
     quit
     ```

   - If the FTP application does not support **`mget`** command, enter:

     ```
     bin
     cd pub
     dir
     get <name of the backup file>
     quit
     ```

     For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

   The system closes the ftp session.

8. To confirm that the backup file, for example, `full_*.tar.gz` is present, enter `dir full_*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Preparing the new servers

- Install both the staged servers to the data equipment rack. The new servers can be one of the following server type:
  - S8800 Server. For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ® Communication Manager* (03-603444).

- Dell™ PowerEdge™ R610 Server.

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

- Apply power to both the servers. Do not turn on the servers.
- Do not connect the servers to any network.
- Do not connect the server duplication cable until instructed.

Complete the upgrade procedures on the staged servers.

Complete the procedures starting from Inserting Communication Manager CD on page 591 through Completion tasks on the staged server on page 601 on the first staged server running Communication Manager release 5.2.1 first. Repeat the procedures on the second staged server running Communication Manager release 5.2.1.

Staging the new servers to Communication Manager Release 5.2.1

Inserting Communication Manager CD

1. Open the CD-ROM drive on the server.
2. Insert the Communication Manager software distribution CD in the CD/DVD drive and close the drive door.

Turning on the server

1. Plug one end of the power cord into the back of the power supply and the other end into a UPS or nonswitched outlet.

   Approximately 5 seconds after the server is connected to power, one or more fans might start running to provide cooling, and the power-on LED blinks quickly (3 flashes per second). Approximately 30 seconds after the server is connected to power, the power-on LED blinks slowly (1 flash per second), and one or more fans might start running to provide cooling.

Note:

Wait for the power-on LED to blink slowly (1 flash per second) before you press the power button. If you press the power button while the power-on LED is blinking quickly (3 flashes per second), the server will not turn on.

2. Press the power button on the front of the server.

   On the server, when the power-on LED (Green) is lit, but does not flash, it indicates that the server is turned on. The power-on LED can be in one of the following states:

   - Off: AC power is not present, or the power supply or the LED itself has failed.
   - Flashing rapidly (3 times per second): The server is turned off and is not ready to be turned on. The power-control button is disabled. This will last about 30 seconds.
   - Flashing slowly (once per second): The server is turned off and is ready to be turned on. You can press the power-control button to turn on the server.
   - Lit: The server is turned on.

   Note:

   - S8800 Server takes longer time to boot than other servers. It can take over five and half minutes for the server to begin to load the software contained on the CD.
   - Do not connect the S8800 server to the network.

   The power-on LED stops blinking and stays lit. After you press the power button, the server takes approximately 5 minutes to initialize.

Connecting the laptop to the server port

1. Connect the laptop to the Services port on the back of the server with a cross-connect CAT5 cable.
2. On your laptop computer, click **Start** > **Run** to open the Run dialog box.
3. Enter ping `-t 192.11.13.6` and press `Enter` to check connectivity between the Services laptop and the server.

Installing Communication Manager Release 5.2.1

Prerequisites

Insert the CD-ROM for Communication Manager Release 5.2.1 into the drive of the server.

1. On your laptop, click **Start** > **Run**.
2. In the Run dialog box, enter `telnet 192.11.13.6` and press `Enter`.

   To navigate on the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install**, highlight **OK** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.
5. When the system prompts you, on the Select Server Mode dialog box, select DUPLEX.
6. When the system displays the message `Private Control Network configuration using both Control Network A and Control Network B?`, select `Yes`.

   When you select Yes, the system performs a hardware check on the server to confirm if six Ethernet interfaces are available on the server. If all six Ethernet interfaces are not available, the installation will fail. The default selection is No.

   The installation process:

   - Partitions and reformats the hard drive and internal compact flash of the server.
   - Installs the Linux operating system.
   - Installs Communication Manager and reports the progress.

   The installation process takes about 20 minutes. When the server is ready to reboot, the CD/DVD drive door opens and a reminder to check the Avaya Support Site, http://support.avaya.com for the latest software and firmware updates appears on the screen. Remove the CD from the drive.

   The reboot takes about 5–8 minutes. The Telnet session ends automatically.

Checking the reboot progress

1. On the laptop, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
   - The system displays the command line prompt if the cache is cleared.
   - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

   The -t causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying files to the server

Use this procedure to download the following files.

- The latest available service pack for Communication Manager release 5.2.1. Obtain the service pack files from the Avaya Support Web site at http://support.avaya.com.
- The license for Communication Manager release 5.2.1
- Avaya authentication file for Communication Manager release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager release 5.2.1
- The backup data sets from the original server. The data set can be a full backup (`full_*.tar.gz`), the three-part backup set (`os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`) or `upgrade-2.0_*.tar.gz`, if the original server is running Communication Manager release 1.x.

1. Under **Miscellaneous**, click **Download Files**.
2. Click **Browse** to open the **Choose File** window on your computer.
3. Select the files that you need to copy to the server and click **Open**.

You can select four files at a time.

4. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     ii. Click **Yes**.
3. Click **Continue**.

   Note:
   Do not install the preupgrade service pack until instructed.

Verifying the process status

1. Under **Server**, click **Process Status**.
2. Under **Frequency**, select Display Once.
3. Click **View**.
4. Verify that the system displays:
   - `dupmgr` is `Down`.
   - All other operations are `UP STANDBY`.

Setting date, time, and time zone

1. Click **Administration** > **Server (Maintenance)**.
2. Under **Server**, click **Server Date/Time**.
3. Change the date, time, and time zone as needed.
4. Click **Submit**.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Creating a super-user login

Note:

The craft level login can create a super-user login.

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

   Note:
   Ensure that the customer can change this login, its password, or its permissions.

2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**
   The system displays the Administrator Accounts page.
3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.
   The system displays the Administrator Logins -- Add Login: Privileged Administrator page.
5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

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

9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.
    The system informs you the login is added successfully.

Installing the Communication Manager license and authentication files

Caution:

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 111.

If the system displays any of the following messages during the installation, ignore them:

- `Filesync of new license to standby server failed.`
- `Filesync of new certificates to standby server failed.`
- `Filesync failed.`
- `License serial number mismatch.`

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.
   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.
   The system displays a message indicating that the license is installed successfully.
3. Click **Restart CM**.
4. Under **Server**, click **Process Status**.
5. Under **Frequency**, select Display Once.
6. Click **View**.
7. Verify that:
   - `dupmgr` is `Down`.
   - All other operations are `UP`.
8. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.
   The system displays the Authentication File page.
9. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.
   The system displays a message indicating that the authentication file is installed successfully.

Restoring server data

Prerequisites

- Ensure that the license file is valid.

  Note:
  You do not need a license file for survivable core server and survivable remote server.

- Copy the datasets to the server.
- Install the latest service pack for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Depending on the release of Communication Manager of the existing system, the data you restore comes from:

- The three-part backup (os, security, xln) or a full backup
- The backup files copied to the flashcard or the laptop

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - If the backup file is copied to the laptop, click **Local Directory**.

     The fields displays the default directory `/var/home/ftp/pub`. Keep the default directory.

   - If the backup file is copied to the flashcard, click **Local CompactFlash Card**.
3. Click **View**.
4. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
5. Select both **Force** options.
6. Click **Restore**.
7. To view the status of the restore process:
   a. Click **Restore History** and select the file you want to restore.
   b. Click **Status**.
   When the restoration is complete, the system displays the message `backup: 0: restore of <filepath/filename> completed successfully.`

Result

You may lose connectivity between the laptop and the server. Ignore this condition and proceed to the next steps.

Rebooting the server

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Shutdown Server**.
2. Select the following check boxes:
    - **Restart server after shutdown**
    - **Shutdown even if this is the active server**
3. Click **Shutdown**.
   The system displays the `A server shutdown has been requested` message.

Completion tasks on the staged server

1. Log off from System Management Interface.
2. Close the Web browser.
3. Disconnect the laptop from the staged server.

Upgrade tasks on the first staged (Release 5.2.1) Server

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type **`192.11.13.6`**.
4. In the Protocol area, click **SSH**.
5. In the Port field, type **`10022`**.
6. Click **Open**.

   Note:
   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the servers host key and display the PuTTY window.
8. Log on as **craft** or **dadmin**.
9. Type **`Exit`** and press **Enter** to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.

3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Identifying the Ethernet interface

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.

3. Select **Configure all services using the wizard** and click **Continue**.
4. On the Set Identities screen, identify the Ethernet interface assigned to Server Duplication.

   This assignment does not persist throughout the upgrade to Release 6.0.x. However, you must know the assignment to complete the staging of the servers on the Communication Manager Release 5.2.1.

Connecting the server duplication cable to the first staged server

Connect the crossover Ethernet cable to the Ethernet port assigned for server duplication on the first staged server.

Important:

Do not connect the other end of the Ethernet cable to the second server until instructed.

Verifying system status

1. Under **Server**, click **Status Summary**.
2. Verify that `Mode` is `Active`.

   If the `Mode` is `BUSY OUT`, release the server. The server goes to the `Active` mode.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Completion tasks on the staged server

1. Log off from System Management Interface.
2. Close the Web browser.
3. Disconnect the laptop from the staged server.

Upgrade tasks on the second staged (Release 5.2.1) Server

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type `192.11.13.6`.
4. In the Protocol area, click **SSH**.
5. In the Port field, type `10022`.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the servers host key and display the PuTTY window.
8. Log on as **craft** or **dadmin**.
9. Type **`Exit`** and press **Enter** to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing System Management Interface

Use this procedure only if the server is not connected to the network.

1. Open a compatible Web browser.
2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying system status

1. Under **Server**, click **Status Summary**.
2. Verify that `Mode` is `BUSY OUT`.
3. If the `Mode` is `Active`, perform the following steps:
    a. Log on to the server using PuTTy configured for SSH.
    b. Enter `stop -acf`.
    c. Enter `server -b`.
    d. Enter `start -ac`.
    e. Enter `exit` to log off and close PuTTY.
4. Repeat steps 1 through 3 to verify if the `Mode` is `BUSY OUT`.

Identifying the Ethernet interface

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. On the Set Identities screen, identify the Ethernet interface assigned to Server Duplication.

   This assignment does not persist throughout the upgrade to Release 6.0.x. However, you must know the assignment to complete the staging of the servers on the Communication Manager Release 5.2.1.

Connecting the server duplication cable to second staged server

Prerequisites

One end of the Ethernet cable connected to the first server.

Connect the other end of the Ethernet cable to the Ethernet port that is assigned for server duplication on the second server.
The crossover Ethernet cable now connects the two servers.

Verifying the connection for server duplication

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, click **Other server via duplication link**.
3. Click **Execute Ping**.
   If the two endpoints are connected, the system displays, `MessRecv`: `1`.
4. Under **Server**, click **Status Summary**.
   a. Verify that this server is in `BUSY OUT` mode.
   b. Verify that the other server is in `Active` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link`: `up`.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

At this point, the first server is active mode and the second server is busied out.

Completion tasks on the staged server

1. Log off from System Management Interface.
2. Close the Web browser.
3. Disconnect the laptop from the staged server.

Upgrade tasks on the first staged (Release 5.2.1) Server

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type `192.11.13.6`.
4. In the Protocol area, click **SSH**.
5. In the Port field, type `10022`.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the servers host key and display the PuTTY window.

8. Log on as **craft** or **dadmin**.
9. Type `Exit` and press **Enter** to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Starting a SAT session

Prerequisites

Log on to the services port from a directly connected laptop.

1. Perform one of the following:
   - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
   - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

License error message

While you log on to the server using SAT, if you see the following message, ignore it:

```
License-Error: Reference IPSI or Media-Gateway Not Responding System Administration
Will Be Blocked in Approximately _ hours Contact Your Service Representative
Immediately
```

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp]` or `[all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

  Note:
  If this operation fails, follow the escalation procedures before you continue with the next step.

SAT error message

SAT screen displays `Success` message with Error Code `0`.

If SAT screen displays `Cannot access the standby Server at this time`, do not proceed. This error indicates that server duplication is not functional.

Resetting the system

1. Start a SAT session.
2. Log in to the server.
3. Enter `reset system 4` and press **Enter**.
   The system initializes Communication Manager on the release 5.2.1 translations.
4. Wait for Communication Manager to restart.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Completion tasks on both the staged (Release 5.2.1) servers

Complete the procedures starting from Installing the preupgrade service pack on page 115 through Completing duplication cable connections on staged servers on page 616 on the first staged server running Communication Manager release 5.2.1 first. Repeat the procedures on the second staged server running Communication Manager release 5.2.1.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
    - If the status of the update file you want to activate is packed:
        i. Select the **Update ID** and click **Unpack**.
        ii. Wait until the system displays the message, `... unpacked successfully`.
    - If the status of the update file you want to activate is unpacked:
        i. Select the **Update ID** and click **Activate**.
        ii. The system displays the status as the update progresses. The system automatically reboots, if required.
        iii. Click **Yes**.
3. Click **Continue**.

Enabling FTP service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. For **FTP Server**, select **Enable**.
   This step enables FTP service on the local server. FTP service remains enabled for 15 minutes and automatically gets disabled.

Backing up the files to localhost

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:

- In the **User Name** field, enter `anonymous`.
- In the **Password** field, enter `2` or `@`.
- In the **Host Name** field, enter `localhost`.
- In the **Directory** field, enter `/pub`.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Transferring files to the services laptop using FTP

Log on to the services laptop.

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you want to save the backup file.

   Note the name of the directory, you will need it later in the procedure.
4. Enter `ftp 192.11.13.6`.
5. At the `User` prompt, enter `anonymous`.
6. At the `Password` prompt, enter the password.
   For example, `technician@companyname.com`.
7. At the `ftp` prompt:
   - If the FTP application supports the **`mget`** command, enter:

     ```
     bin
     cd pub
     mget migration-60*
     y
     quit
     ```

- If the FTP application does not support **mget** command, enter:

  ```
  bin
  cd pub
  dir
  get <name of the backup file>
  quit
  ```

  For example, `migration-60_cmserver_172731_20100516.tar.gz`.

The system closes the ftp session.

8. To confirm that the backup file, for example, `migration-60*.tar.gz` is present, enter `dir migration*`.
   If the backup file is present, proceed with the next steps of the upgrade procedure.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Completing duplication cable connections on staged servers

1. Disconnect the server duplication cable.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

   Note:
   Do not connect the staged servers to the network.

Upgrade tasks on both the S8800 (Release 6.0.1) Servers

Complete the procedures starting from Installing System Platform and Communication Manager on page 150 through Rebooting the server on page 125 on the first staged server running Communication Manager Release 6.0.1 first. Repeat the procedures on the second staged server running Communication Manager Release 6.0.1.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Communication Manager Messaging file.

  Note:
  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the new server

1. Do not connect the server to the network until you are instructed to do so.
2. Connect the server duplication Ethernet cable to the service port labeled **4** on both the staged servers.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

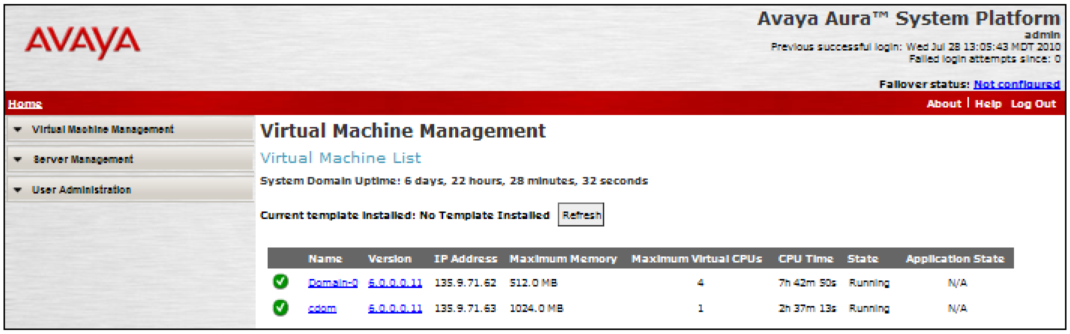
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.


AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

Use this procedure to copy the service packs or the upgrade data set (for example, migration-60*.tar.gz file) to the server.

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:
You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.

    - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
  - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade to duplex template - worksheet on page 1347.

On the System Management Interface, under, **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the staged servers running Release 6.0.1

Starting a SAT session

Prerequisites

Log on to the services port from a directly connected laptop.

1. Perform one of the following:
   - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
   - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Busying out the standby server

Prerequisites

Log on to System Management Interface of the standby server.

Busyout the standby server.

1. Log in as `craft` or `dadmin`.
2. Under **Server**, click **Busy-Out/Release Server**.
3. Click **Busy Out**.

Tasks on the first staged Release 6.0.1 server (active)

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the connection for server duplication

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, click **Other server via duplication link**.
3. Click **Execute Ping**.
   If the two endpoints are connected, the system displays, `MessRecv`: `1`.
4. Under **Server**, click **Status Summary**.
   a. Verify that this server is in `Active` mode.
   b. Verify that the other server is in `BUSY OUT` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link`: `up`.

Completion tasks on the standby S8700 Server

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type **`192.11.13.6`**.
4. In the Protocol area, click **SSH**.
5. In the Port field, type **`10022`**.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the servers host key and display the PuTTY window.
8. Log on as **craft** or **dadmin**.
9. Type **`Exit`** and press **Enter** to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.

3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Completion tasks on the active S8700 Server

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type `192.11.13.6`.
4. In the Protocol area, click **SSH**.
5. In the Port field, type `10022`.
6. Click **Open**.

Note:

If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.

7. Click **Yes** to accept the servers host key and display the PuTTY window.
8. Log on as **craft** or **dadmin**.
9. Type `Exit` and press **Enter** to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Important:

Service outage begins at this point of the upgrade process.

Postupgrade tasks on the first staged Release 6.0.1 server (active)

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Verifying the Communication Manager operation

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Administering the node name for server A for each duplex survivable core

Prerequisites

Start a SAT session.

Complete this task on the main server only.

Perform this task after you upgrade an S8700-Series main server from Communication Manager releases earlier than 5.2.1 to Release 5.2.1 or later; and if the main server has administered survivable servers of type “ESS D” as observed on the **`list survivable-processor`** screen.

During the upgrade, the system performs the following actions on the upgraded main server:

- Transfers the server A node name on the System Parameters ESS SAT screen of the preupgrade main server to the **ACTIVE SERVER IP Address** field on the Survivable Processor screen of the upgraded main server.
- Sets the **SERVER A Node Name** field on the Survivable Processor screen to blank. Because of this action, ESS alarm 799 is generated on the main server.

1. Enter `list survivable-processor` and search for “ESS D” to locate the servers that need administering.
2. Enter `change survivable-processor New-node-name`, where, New-node-name is the node name assigned to the survivable core server.

   You can determine the node name from the list survivable-processor screen.
3. Administer the node name of the ESS server A.
   The alarm clears after the Server A node name is administered for the duplex survivable core server.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:

   i. Click **Change**.
   ii. On the Change Current Schedule Web page, click **Change Schedule**

- To remove the schedule backup, click **Remove**.

  The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Postupgrade tasks on the second staged Release 6.0.1 server (busied out)

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:

  i. Click **Change**.
  ii. On the Change Current Schedule Web page, click **Change Schedule**

- To remove the schedule backup, click **Remove**.

  The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.
   The roles of the active and standby servers changes.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8700-Series servers to S8800 servers

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 on S8700-Series servers to Release 6.0.1.

In this upgrade procedure, you replace the S8700-Series servers with S8800 Servers running System Platform and the duplex main/survivable core template.

Note:

Beginning from Release 6.0.1, Communication Manager supports upgrading to Dell™ PowerEdge™ R610 Servers and HP ProLiant DL360 G7 Servers in addition to S8800 Servers.

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Overview on page 1375.

- For Communication Manager Release 3.0 and later, perform the conversion before you upgrade the servers.
- For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8700-Series servers to Communication Manager Release 4.0.5 or Release 5.2.1.
    - For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).
    - For S8700 servers, see *Upgrading Servers to the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603445).
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.0.1.
3. Perform the upgrade to Release 6.0.1 as described in this section.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.0.1:

- The main server
- The survivable core server (formerly enterprise survivable servers)

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	

✔	Task	Description
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade:

✔	Task	Description
	Verify that you have the required software. • System Platform • The Communication Manager template	

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information on how to accomplish this task, and about specific commands, see:

- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431)
- *Avaya Aura™ Communication Manager Server Alarms* (03-602798)

Preupgrade tasks on the active S8700-Series server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.

2. Verify that the **CM Reports as:** field displays one of the following:

   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.
      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**
    - **Set Identities**
    - **Configure Interfaces**
    - **Set DNS/DHCP**
    - **Set Static Routes**
    - **Configure Time Server**
    - **Server Access**
    - **Server Date/Time**
    - **Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

Full Backup does not backup voice mail configurations or messages.

3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > **Caution:**
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

     > **Note:**
     > For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:
     >
     > - **Avaya Call Processing (ACP) Translations**
     > - **Server and System Files**
     > - **Security Files**

   - If Communication Manager Messaging is enabled:

     i. Select **Specify Data Sets**.

ii. Select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**
- **Communication Manager Messaging (CMM)**

Select **Translations, Names, and Messages**.

iii. In the **Download size** field, enter the size of the backup `.tar` file.

There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Converting fiber PNs to IP-PNC

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Overview on page 1375.

Note:
For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

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

```
Backup successful
```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Preupgrade tasks on the standby S8700-Series server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.

2. Verify that the **CM Reports as:** field displays one of the following:

   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:

    i. Select **Specify Data Sets**.

    ii. Select the following check boxes:

    - **Avaya Call Processing (ACP) Translations**
    - **Server and System Files**
    - **Security Files**
    - **Communication Manager Messaging (CMM)**

      Select **Translations, Names, and Messages**.

    iii. In the **Download size** field, enter the size of the backup `.tar` file.

    There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**. Enter the host IP address.
    - **Directory**

    When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

Caution:

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.

   ii. Wait until the system displays the message, `... unpacked successfully`.

- If the status of the update file you want to activate is unpacked:

   i. Select the **Update ID** and click **Activate**.

   ii. The system displays the status as the update progresses. The system automatically reboots, if required.

   iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
3. Click **Submit**.

    The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**
    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Removing the duplication cable

1. Label and disconnect the duplication fiber cable (if present) from the server.
2. Label and disconnect the duplication interface IP cable from the server.

Removing the server from the rack

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.

3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Installing both S8800 servers in the rack

Install the S8800 servers in the rack. For more information, see *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603444).

At this point do not connect the servers to any network.

Upgrade tasks on the first S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:

If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the server

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

   Important:

   Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.

b. Log in to System Domain (Domain-0) as admin.

c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

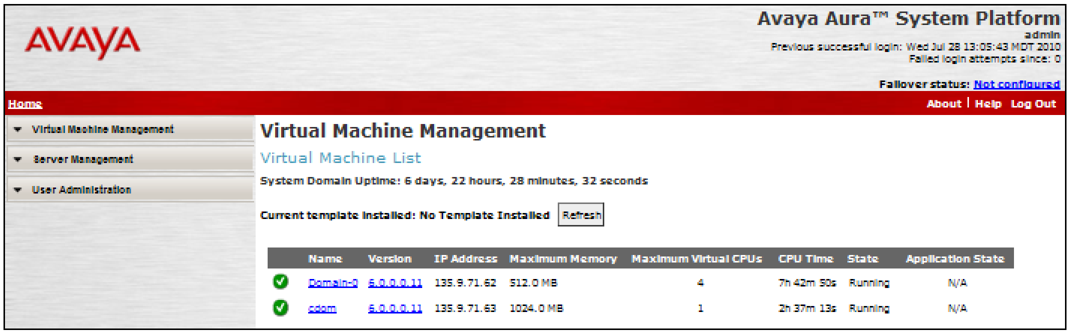
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade to duplex template - worksheet on page 1347.

On the System Management Interface, under, **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying connectivity

To verify if the Ethernet port is working, ping the FTP server, where you saved the backup files.

1. Under **Diagnostics**, click **Ping**.
2. Complete one of the following:
   - If the system has IPSIs configured on it, select the IPSIs and the cabinet numbers.
   - In the **Host Name or IP address** field, enter the IP address of the device on which you stored the backup files.
3. Click **Execute Ping**.
   If the ping fails, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300432).

On the active S8700 server

Completion tasks on the active S8700 server

You need to perform the following two procedures on the active S8700 server.

Important:

After you complete these two tasks, at this point, the service will be down as both the S8700 servers are shutdown. To minimize the downtime, shut down the active S8700 server, access the first S8800 server again and release the server immediately.

You must then move to the S8800 server and continue with the upgrade procedures.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Removing the server from the rack

1. Label and disconnect all remaining cables.
2. Disconnect the laptop from the Services port.
3. Disconnect the power cord from the UPS.
4. Disconnect USB flashcard reader or writer.
5. Disconnect any modem.
6. Remove the server from the rack, if necessary.
7. Remove the rails from the rack.

Postupgrade tasks on the first S8800 Server

Accessing the S8800 server

1. Clear the ARP cache on the laptop, if necessary.
2. Open a Web browser and connect to the server.
3. Log on to the server using System Management Interface.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Reset the settings that you recorded Disabling scheduled maintenance on page 37.

Saving translations

Perform this procedure on the main server only.

Enter `save translation all`.
The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
    - To change the schedule backup:
        1. Click **Change**.
        2. On the Change Current Schedule Web page, click **Change Schedule**
    - To remove the schedule backup, click **Remove**.

      The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.

3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
    - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
    - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

    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.
4. Select where to store or send the backup files:
    - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
    - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
    - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

        Note:

        Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Upgrade tasks on the second S8800 Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

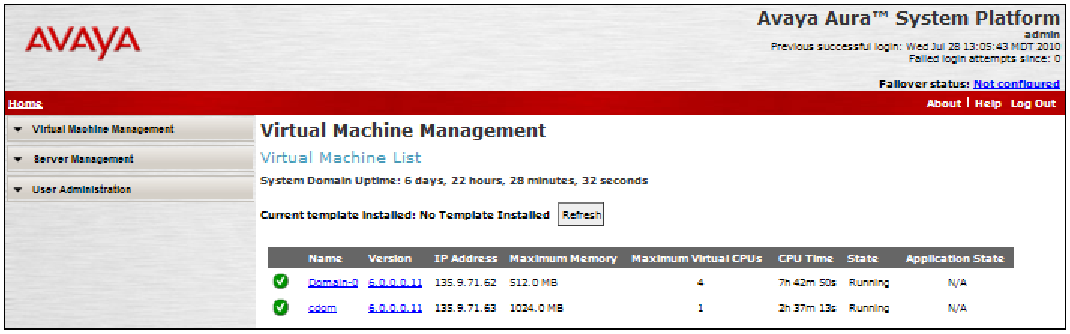
   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.

4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Avaya Aura™ System Platform

admin

Previous successful login: Wed Jul 28 13:05:43 MDT 2010

Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:

- **Avaya Downloads (PLDS)**
- **HTTP**
- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Connecting the cables to the server

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

   Important:
   Do not release the server until instructed.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you

plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**

- **Host Name**
- **Directory** or **Field Path**
  - If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade simplex to duplex template - worksheet on page 1359.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.

The roles of the active and standby servers changes.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8800 Server to S8800 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 on duplex S8800 Servers to Release 6.0.1 using System Platform and the duplex main/ survivable template on Avaya S8800 Servers.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following additional tasks to reuse the existing server:

- Increase the memory
- Add a third hard drive
- Update the uEFI firmware
- Reconfigure the RAID controller to support RAID 5
- Update the uEFI settings

> **Note:**
> For instructions to update the uEFI firmware and uEFI settings, download the release notes for Release 6.0.1 from the Avaya Support Web site at http://support.avaya.com.

For more information, see the *Avaya S8800 Migration Kit*.

Use this section to upgrade:

- The main server
- The survivable core server (formerly enterprise survivable server)

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that private control networks for IPSI connectivity to the server are removed before you run a preupgrade backup.	For instructions, see Introduction on page 1371.
	Ensure that you have the upgrade-specific hardware on hand.	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Preupgrade tasks

Onsite upgrade checklist

When you are onsite, complete the following tasks before you start the server upgrade.

✔	Task	Description
	Verify that you have the required software. • System Platform • Communication Manager template	
	Verify that you have all the necessary equipment onsite, for example: • Hard disk drive • Memory module • Services laptop and crossover cable • Electrostatic wrist ground strap and mat	For the list of required equipment, see *Avaya Migration Kit.*
	Obtain the CD to update the uEFI firmware using one of the following ways: • Order the uEFI firmware CD • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.	
	Obtain the RIAD 5 firmware CD	
	Obtain the CD to update the uEFI settings using one of the following ways: • Order the uEFI settings CD • Download the `S8800uEFITool.iso` file	

✔	Task	Description
	from Avaya Support Site and create a CD.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Survivable core servers resetting

The survivable core server might take over during the server upgrade. Plan on a failover to survivable core server or survivable remote server, if present, in the configuration during the upgrade of the main server.

For more information on how to accomplish this task, and about specific commands, see:

- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431)
- *Avaya Aura™ Communication Manager Server Alarms* (03-602798)

Preupgrade tasks on the active S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:

a. Right-click and select **Paste**.

   The configuration screen appears in your application window.

b. Click **File** and select **Save As**.

c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging in from a laptop directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp] or [all or ess or lsp]`, enter `save translation all`.
- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - Select **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     1. Select **Specify Data Sets**.
     2. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
3. In the **Download size** field, enter a value that determines the size of the `.tar` file backed up.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

Caution:

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.

    ii. Wait until the system displays the message, `... unpacked successfully`.

- If the status of the update file you want to activate is unpacked:
    i. Select the **Update ID** and click **Activate**.
    ii. The system displays the status as the update progresses. The system automatically reboots, if required.
    iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
3. Click **Submit**.

    The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**
    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Verifying the hardware on the server

Verify the memory, hard drive, and RAID configuration on the existing server:

1. Log on to System Management Interface and select **Administration** > **Server (Maintenance)**.
2. Under **Server Configuration**, select **Display Configuration**.
3. Under **Disk devices**, verify if the system has three 146GB hard disk drives. If the system does not have three disk drives, install a disk drive on the server later when you are instructed to do so.

Disconnecting the cables

1. Label and disconnect the power cord(s) from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Preupgrade tasks on the standby S8800 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays `R015x.02.1.016.4`.

   This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:

   a. Right-click and select **Paste**.

      The configuration screen appears in your application window.

   b. Click **File** and select **Save As**.

   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

   d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.

7. Print or copy the information from the following screens:

   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.

9. On the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for product ID.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.
   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   > ⚠ **Caution:**
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:

- If Communication Manager Messaging is not enabled:

  Select **Full Backup**.

  The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

  > **Note:**
  > For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:
  >
  > - **Avaya Call Processing (ACP) Translations**
  > - **Server and System Files**
  > - **Security Files**

- If Communication Manager Messaging is enabled:

  i. Select **Specify Data Sets**.

  ii. Select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
  - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.

  iii. In the **Download size** field, enter the size of the backup `.tar` file.

  There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.

6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   > **Note:**
   >
   > ***Do not*** select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

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

```
Backup successful
```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Verifying the hardware on the server

Verify the memory, hard drive, and RAID configuration on the existing server:

1. Log on to System Management Interface and select **Administration** > **Server (Maintenance)**.
2. Under **Server Configuration**, select **Display Configuration**.
3. Under **Disk devices**, verify if the system has three 146GB hard disk drives. If the system does not have three disk drives, install a disk drive on the server later when you are instructed to do so.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.

4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the cables

1. Label and disconnect the power cord(s) from the power supply at the back of the server.
2. Label and disconnect the Ethernet cables from the dual NIC at the back of the server.

Removing the server cover

Prerequisites

Before you disconnect the server from the power source, make a note of which LEDs are lit, including the LEDs that are lit on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs are not lit when the power source is removed.

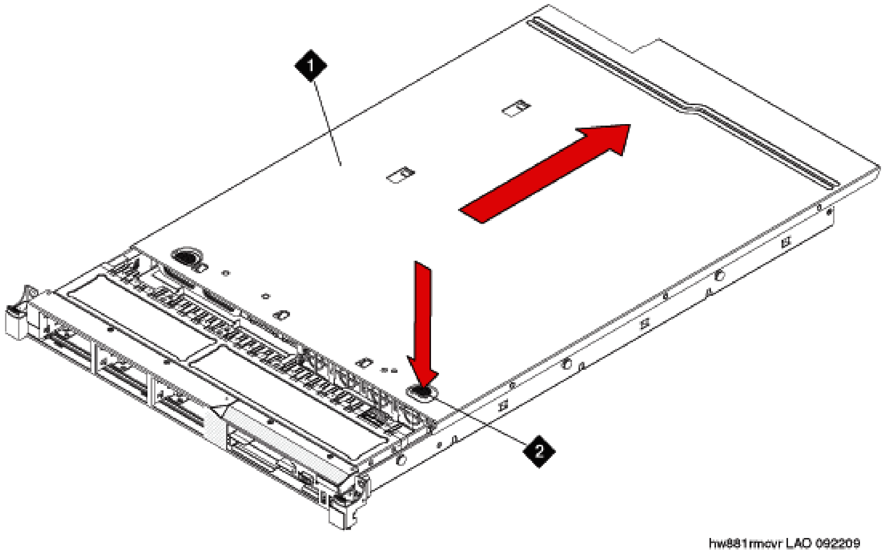
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
   a. Turn off the server and all attached devices.
   b. Label and disconnect all power cords and external cables.

3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

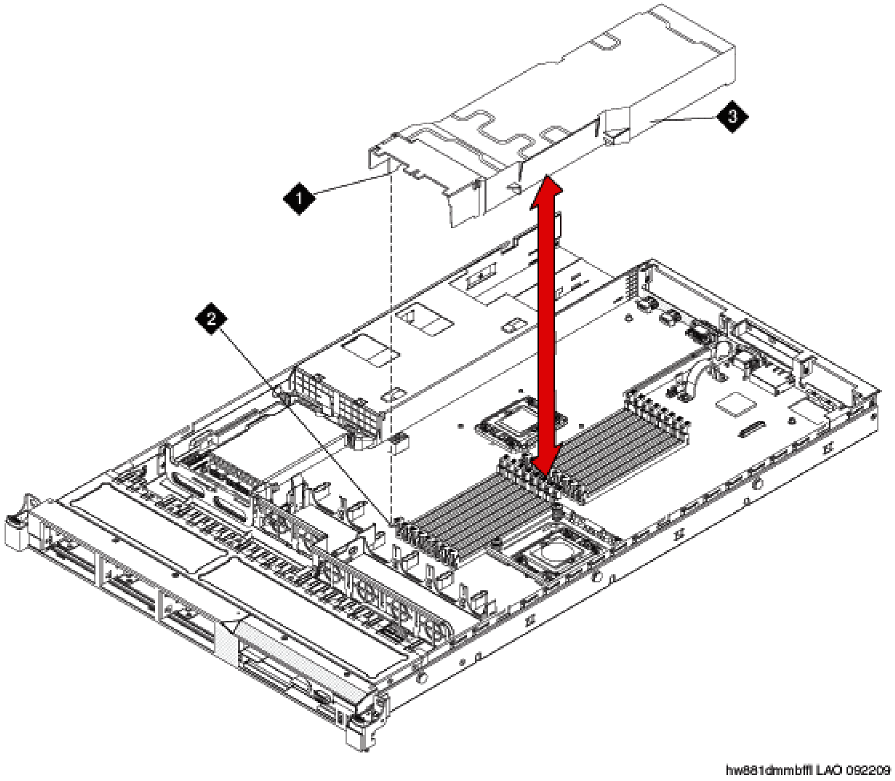
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Grasp the DIMM air baffle and lift the air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Prerequisites

Remove the DIMM air baffle.

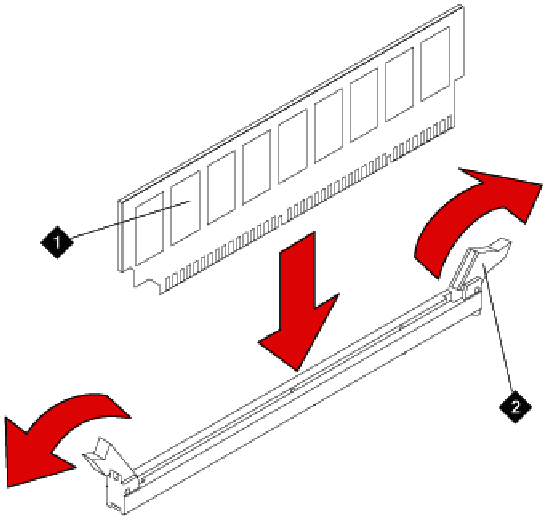
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.

6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.
   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

   Important:

   If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.

7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.
    When you install or remove memory modules, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

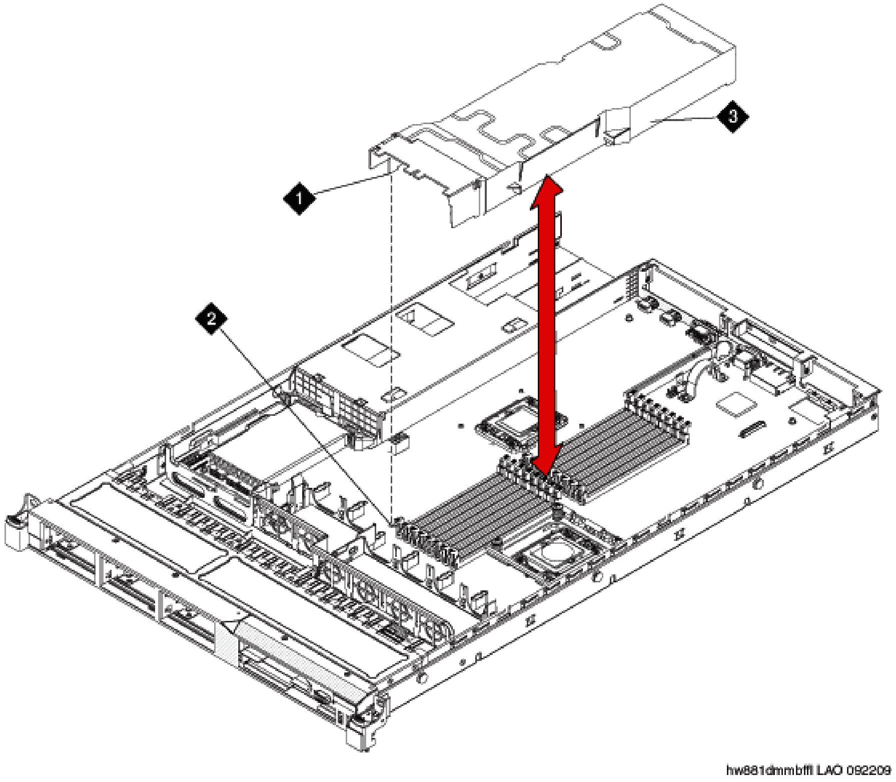
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

Prerequisites

If replacing an existing hard drive, remove the hard drive that you want to replace.

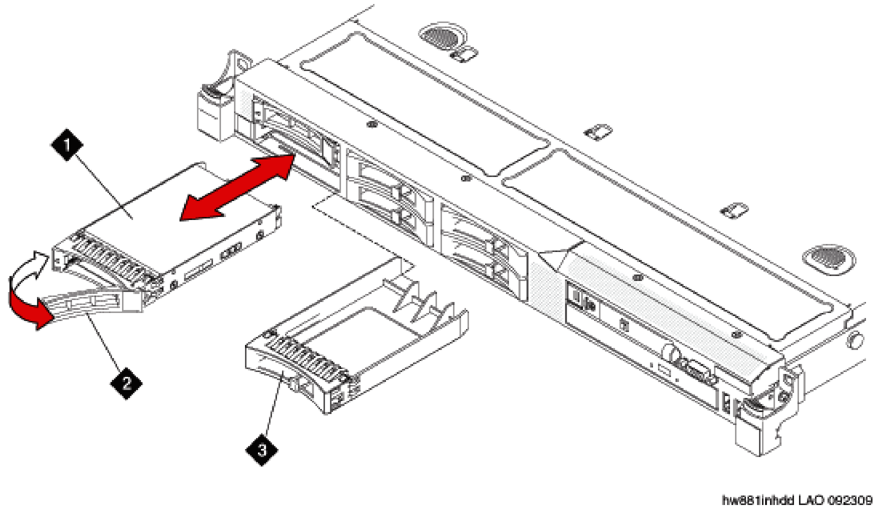
Important:

To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. If the amber LED remains lit, the drive is faulty and must be replaced.

Updating S8800 server firmware

Prerequisites

- Obtain the CD for uEFI firmware. You must either order the CD or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Prerequisites

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.
2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration &
   Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server,

reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Next steps

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

Prerequisites

- Obtain the CD for uEFI settings of S8800 Server. You may order the CD, or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks on the standby server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Communication Manager Messaging file.

  Note:
  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

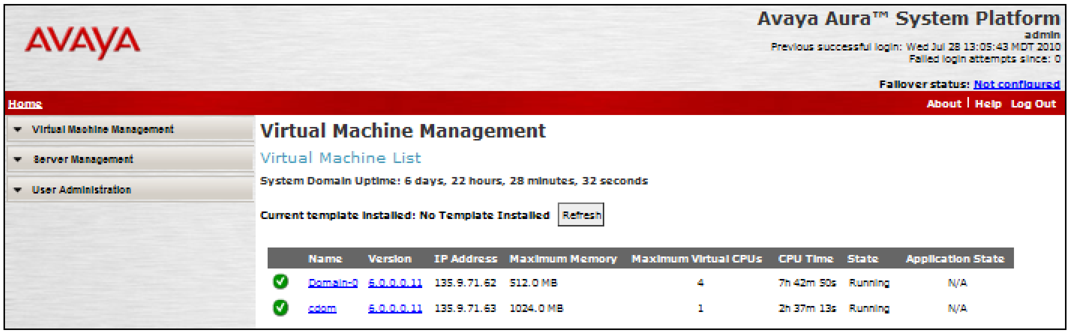
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade to duplex template - worksheet on page 1347.

On the System Management Interface, under, **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Unplug the laptop from the services port.

Tasks on the active S8800 server

Completion tasks on the active S8800 Server

When you shutdown the active S8800 Server as outlined in the following procedure, the service outage begins.

Important:
To minimize the downtime, shut down the active S8800 Server, access the standby S8800 Server and release the server in the shortest amount of time possible.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Upgrade tasks on the standby S8800 Server

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Unplug the laptop from the services port.

Upgrade tasks on the S8800 Server that is shutdown

Removing the server cover

Prerequisites

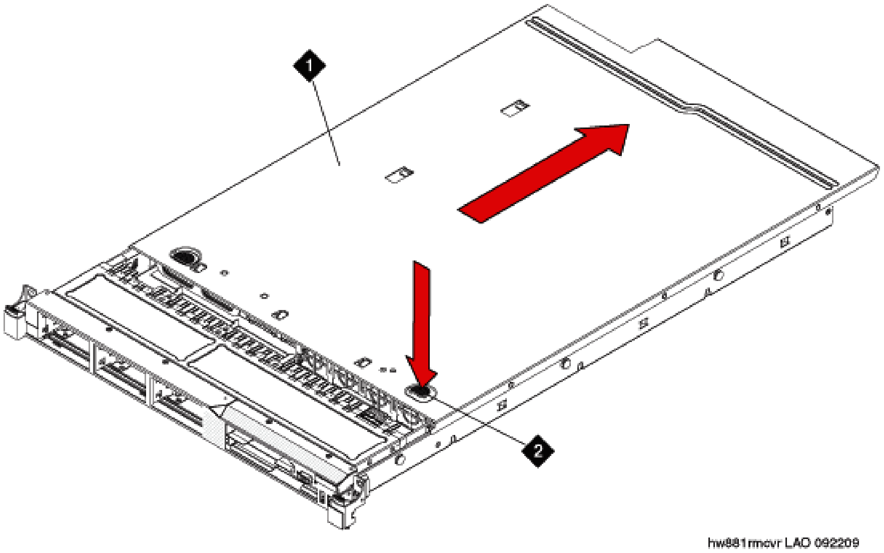
Before you disconnect the server from the power source, make a note of which LEDs are lit, including the LEDs that are lit on the operation information panel, on the light path diagnostics panel, and LEDs inside the server on the system board. Once you disconnect the server from the power source, you lose the ability to view the LEDs because the LEDs are not lit when the power source is removed.

Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. If you are planning to view the error LEDs that are on the system board and components, leave the server connected to power.
2. If you are planning to install or remove a DIMM, PCI card, battery, or other non-hot swap device:
    a. Turn off the server and all attached devices.
    b. Label and disconnect all power cords and external cables.
3. If the server has been installed in a rack, slide the server out from the rack enclosure.
4. Press down firmly on the blue tab on the top (near the front of the server) of the cover and slide the cover toward the back of the server until the cover has disengaged from the chassis. See the following figure.



1	Cover
2	Tab

5. Lift the server cover off the server and set it aside.

Important:

For proper cooling and airflow, replace the cover before you turn on the server. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Adding the memory module

Removing the DIMM air baffle

You must remove the DIMM air baffle to replace or install a memory module.

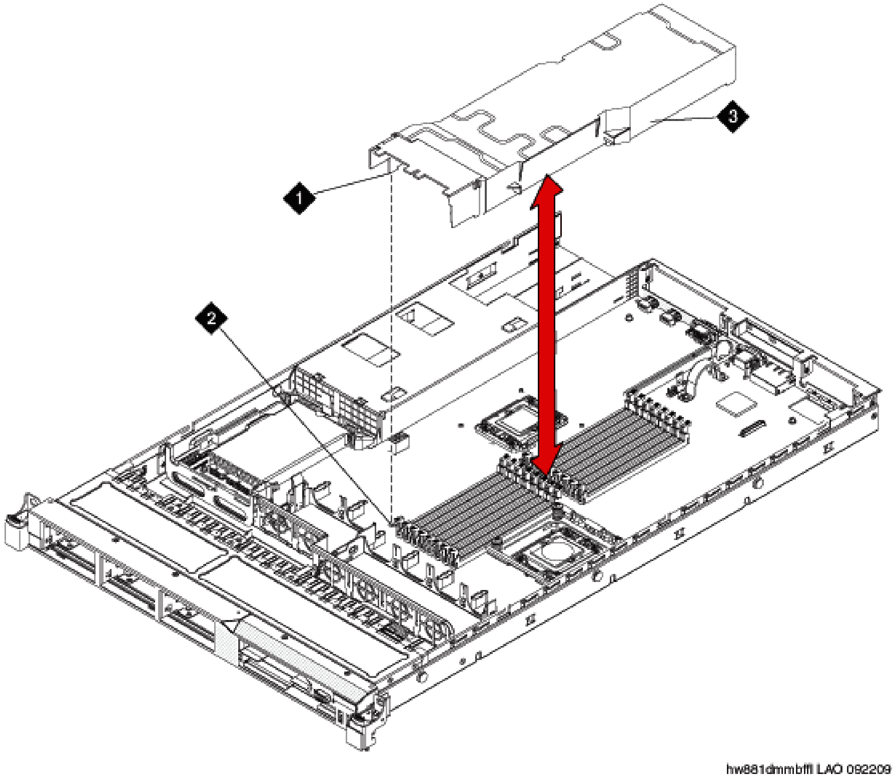
Caution:

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Grasp the DIMM air baffle and lift the air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Installing a memory module

Prerequisites

Remove the DIMM air baffle.

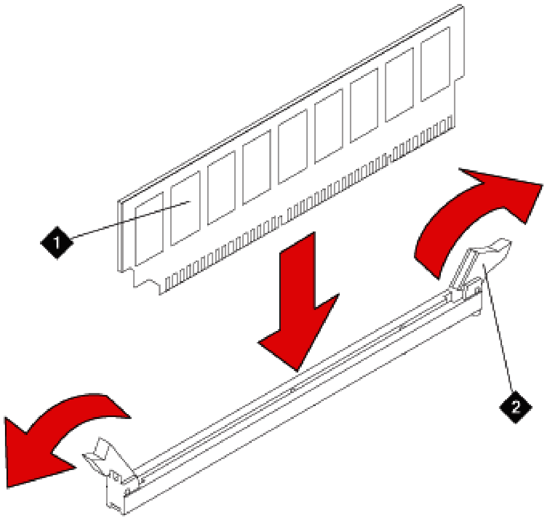
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Carefully open the retaining clips on each end of the memory module connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the memory module connectors.



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.
4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.
   The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

Important:

If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.

7. Replace the air baffle over the memory modules. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.
    When you install or remove memory modules, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

You must install the DIMM air baffle after you install a memory module.

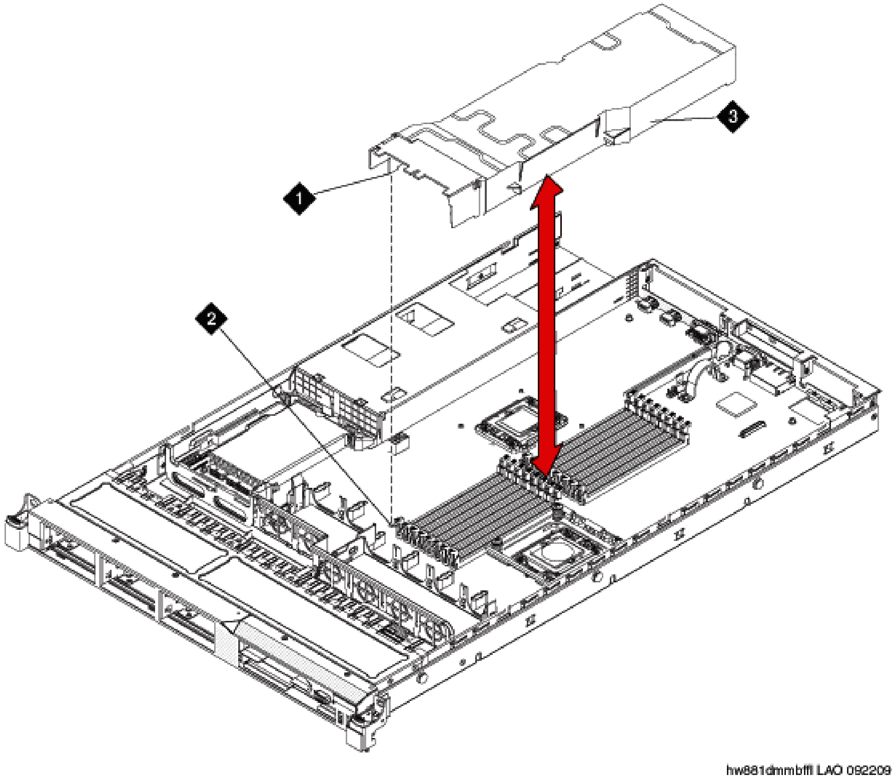
⚠ **Caution:**

For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Installing a hard disk drive

Prerequisites

If replacing an existing hard drive, remove the hard drive that you want to replace.

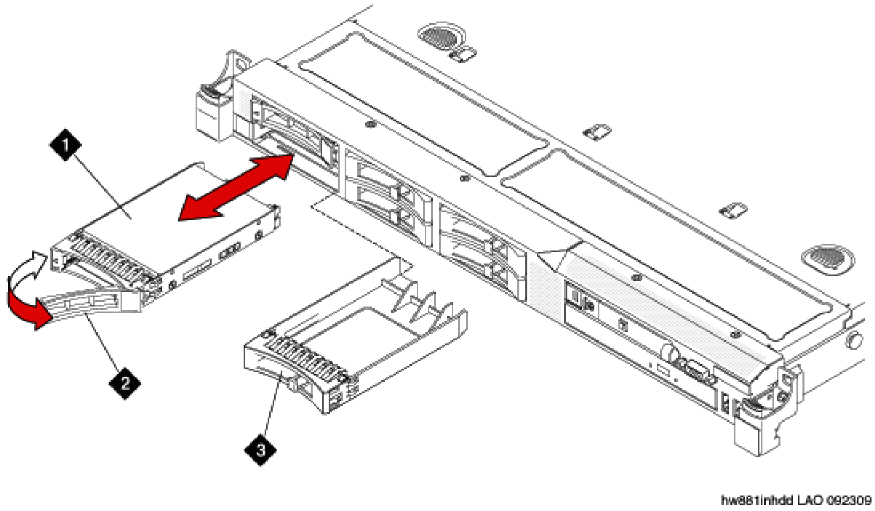
Important:

To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage for more information.

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.
6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. If the amber LED remains lit, the drive is faulty and must be replaced.

Updating S8800 server firmware

Prerequisites

- Obtain the CD for uEFI firmware. You must either order the CD or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Prerequisites

- Obtain the CD for RAID 5 firmware. You must either order the CD or download the `S8800RAIDTool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for configuring the RAID 5 firmware from the Avaya Support Web site at http://support.avaya.com.

Important:

The conversion process destroys any data present on the hard disk drives. Therefore, ensure that you back up any data or translations.

The server, to which you added the third 146 GB hard drive requires conversion from RAID 1 to RAID 5.

1. Insert the RAID 5 firmware CD into the disk drive of the server.

   When the server boots, the scripts runs automatically.

2. Verify that the system configures the RAID successfully. The screen must display the following message:

   ```
   ... 3 Hard Drives Found, Applying Avaya RAID 5 Configuration &
   Settings....
   ```

   The system automatically ejects the CD when it completes the configuration. If the system does not detect all the hard disk drives that you installed on the server,

reboot the server and run the configuration tool again. If the system does not detect after the second attempt, escalate to Avaya Global Support Services or the authorized Avaya Business Partner.

3. Remove the CD from the drive and press `Enter` to reboot the server.

   Alternatively, wait for two minutes, the system reboots automatically.

Next steps

Install the `S8800uEFITool.iso` updates.

Updating uEFI settings

Prerequisites

- Obtain the CD for uEFI settings of S8800 Server. You may order the CD, or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Install the `S8800uEFITool.iso` file on the server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:

If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Communication Manager Messaging file.

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Connecting the cables to the server

1. Connect the server to customer LAN.
2. Perform one of the following:
   - If you are on the first server, do not connect the server duplication Ethernet cable to either server.
   - If you are on the second server, connect the server duplication Ethernet cable to both servers.

   Important:

   Do not release the server until instructed.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.

5. Enter a valid password.
6. Click **Log On**.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

> **Note:**
> If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

> **Note:**
> You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.

  - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
- Click **Local Directory** and provide the path to the backup file on your local directory.

  Important:
  If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade to duplex template - worksheet on page 1347.

On the System Management Interface, under, **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.
   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Unplug the laptop from the services port.

Postupgrade tasks on the active server

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Reset the settings that you recorded Disabling scheduled maintenance on page 37.

Saving translations

Perform this procedure on the main server only.

Enter `save translation all`.
The system displays the `Command successfully completed` or the `all error messages are logged` message.

If the system displays `Cannot access the standby Server at this time`, ignore the message. The system displays this message because the standby server is not upgraded and server duplication is not available at this point.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
    - To change the schedule backup:
        1. Click **Change**.
        2. On the Change Current Schedule Web page, click **Change Schedule**
    - To remove the schedule backup, click **Remove**.

      The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
    - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
    - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Disconnecting from the server

Unplug the laptop from the services port.

Postupgrade tasks on the standby S8800 Server

Connecting the services laptop to the server

Using a CAT5 cable, connect the laptop to the services port.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

  Note:

  Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.
   The roles of the active and standby servers changes.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.

6. Verify that the status for all operations is `UP`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading DEFINITY SI or R Server to the S8800 Server

Introduction

This section describes the procedure to upgrade the following existing DEFINITY Server to Communication Manager Release 6.0.1 on S8800 Servers, Dell™ PowerEdge™ R610 Servers or HP ProLiant DL360 G7 Servers:

- DEFINITY SI Server in an SCC1 or an MCC1
- DEFINITY R Server in an MCC1

In this procedure, you discard the cabinet and move the supported circuit packs to G650 Media Gateway. You install the new servers running System Platform and the duplex main/survivable core template (CM_Duplex).

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing translation file on Communication Manager Release 6.0.1.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

This upgrade affects service. When you turn off the PPN stack to replace the cabinet as part of the upgrade process, the system drops all calls. Service returns when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following server, as appropriate: - S8800 Server	

✔	Task	Description
	- Dell™ PowerEdge™ R610 Server - HP ProLiant DL360 G7 Server • G650 Media Gateway • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP or later C-LAN	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	Installing the Avaya G650 Media Gateway (03-300685)	Provides instructions for installing and configuring the G650 Media Gateway.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PNs to prepare the DEFINITY system for upgrade. The changing or upgrading the hardware includes:

- Changing TN2182 Tone Clock and maintenance circuit packs for TN2312BP IP Server Interfaces (IPSI) and new TN779D maintenance circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service. However, duplex-reliability configurations encounter short service interruptions when you change the tone-clock circuit pack is in IPSI-controlled PNs.

Server and IPSI cable connections

Each IPSI circuit pack must have a CAT5 cable that connects to the customer network. Cables for IPSIs are located in PN carrier A. If the system has a duplicated bearer network, the cables for IPSIs are located in PN carrier B.

In duplex configurations, each server is connected to the customer network that comprise control network A (CNA). If this system has duplicated IPSIs, each server is connected to the customer network that comprise control network B (CNB).

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Replacement of circuit packs

All PNs receive IPSI circuit packs. The TN2312BP IPSI circuit pack replaces the existing TN2182 Tone Clock circuit pack and terminates control communication with the servers. Flat ribbon cables run between the IPSIs and the maintenance circuit pack. These ribbon cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit packs, program static IP addresses into the IPSIs.

You can complete this stage at any time before the cutover. The tone clock and the IPSI circuit packs are hot swappable, and you replace the circuit packs in the existing DEFINITY system without the need to turn off the power.

The IPSI circuit pack provides the same functionality as the tone clock circuit pack. You perform the following tasks before the cutover:

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSIs are working as tone clocks in the existing system.
- Test the connectivity between the server and the IPSI.
- Reinstall the IPSIs in the new carriers after you install the carriers.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Prerequisites

A cross-over cable to connect your services laptop directly to the processor.

1. Perform one of the following tasks to connect the services laptop to the processor:
    - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
    - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

    This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks on both the servers

Installing both the servers in the rack

Install the new servers in the rack. At this point do not connect the servers to any network. For instructions to install the servers in the rack, see the following documents:

- For S8800 Server, see *Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager* (03-603444).
- For Dell™ PowerEdge™ R610 Server, see *Installing the Dell™ PowerEdge™ R610 Server (working title)*.
- For HP ProLiant DL360 G7 Server, see *Installing the HP ProLiant DL360 G7 Server (working title).*

Complete the procedures starting from "Installing System Platform and Communication Manager" through "Rebooting the server" on the first S8800 Server first. Repeat the procedures on the second S8800 Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:
You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

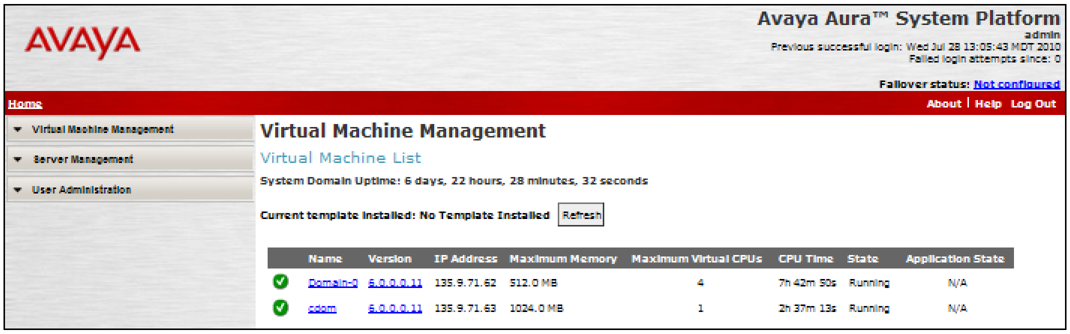
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the translations

Prerequisites

Log in to System Management Interface.

Use this procedure to restore translations only on the main server. When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

1. Under **Administration**, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

   Important:
   If the server is not connected to the network, you must select **Local Directory**.
4. Click **View**.

5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:

   Do not restore a file with a name that starts with a "os_" or "full_". Restore only the files with the extension `.xln`.

6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the Restore status.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Configuring server data

Configure the server data using the worksheets available in Communication Manager upgrade to duplex template - worksheet on page 1347.

On the System Management Interface, under, **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**
- **Duplication Parameters**

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.

3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the S8800 Servers

Starting a SAT session

Prerequisites

Log on to the services port from a directly connected laptop.

1. Perform one of the following:
   - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
   - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Busying out the standby server

Prerequisites

Log on to System Management Interface of the standby server.

Busyout the standby server.

1. Log in as `craft` or `dadmin`.
2. Under **Server**, click **Busy-Out/Release Server**.
3. Click **Busy Out**.

Tasks on the first S8800 Server

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the connection for server duplication

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, click **Other server via duplication link**.
3. Click **Execute Ping**.
   If the two endpoints are connected, the system displays, `MessRecv`: `1`.
4. Under **Server**, click **Status Summary**.
   a. Verify that this server is in `Active` mode.
   b. Verify that the other server is in `BUSY OUT` mode.

   If the mode of the other server is `Not Ready`, it implies that the server duplication is not functional. Do not proceed until the server duplication is functional.

   If the server duplication connection is successful, the system displays, `Duplication Link`: `up`.

Postupgrade administration on both the servers

Connecting a laptop to the server

Prerequisites

Make sure that you have a Secure Shell (SSH) application such as PuTTY installed on your laptop.

1. Connect the laptop to the services port (eth1) using a crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   The system assigns the IP address 192.11.13.6 to eth1 by default. eth1 is the second interface on the server.
2. Start an SSH session.
3. In the Host Name (or IP Address) field, type `192.11.13.6`.
4. In the Protocol area, click **SSH**.
5. In the Port field, type `10022`.
6. Click **Open**.

   Note:

   If you are using PuTTY, the system displays the PuTTY Security Alert window the first time you connect to server.
7. Click **Yes** to accept the servers host key and display the PuTTY window.
8. Log on as **craft** or **dadmin**.
9. Type `Exit` and press **Enter** to close PuTTY.

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.

3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.

4. Enter `exit`.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

   For more information, see About subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing G650 Media Gateway in the rack

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.

3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.
6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.
4. For G650, if the maintenance function is used:
   a. Connect one end of the serial maintenance cable to the DB9 connector on the IPSI adapter.
   b. Connect the other end to the Emergency Transfer panel to provide 1 alarm output and 2 alarm inputs.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Port network circuit packs

Because you do not reuse the PPN after the upgrade, you must:

- Relocate the port network circuit packs to a new G650 Media Gateway.
- Remove all port network circuit pack translations related to the PPN. The STS group manages the translation changes necessary for this upgrade.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.

4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you might also need to adjust the administration of the network regions. Your planning documents might provide information about changes to network regions. For more information on how to administer network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit packs

Prerequisites

Start a SAT session.

Complete Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6

- DiffServ: 46

3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

> **Important:**
> Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

The default is **none**.

Removing fiber-related administration

Prerequisites

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Disabling PNC duplication

If the bearer network is duplicated, remove the duplication before you remove the fiber-optic connections. If the system does not have PNC duplication, continue with the next procedure.

1. To check which of the duplicated PNCs is active, enter `status pnc`.
2. To busyout the standby PNC, enter `busyout pnc-standby`.
3. To open the duplication screen, enter `change system-parameters duplication`.
4. In the **Enable Operation of PNC Duplication** field, enter `n` and click **Submit**.

Administering PN synchronization

Prerequisites

Open a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network` *n*, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

   The system displays a list of all the cabinets and the PNs that the cabinets contain under **Circuit Packs Available for Synchronization**.
5. Obtain a location for the synchronization source circuit pack from the list under **Circuit Packs Available for Synchronization** for **Primary** and **Secondary** fields. Ensure that you choose a working synchronization source.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, add another synchronization-source circuit pack location in the **Secondary** field.
8. Press **Submit**.

   Wait about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization-switch all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must show `PASS` in the **Results** field. If the **Results** field does not show `PASS`, you must troubleshoot the synchronization error.

Disconnecting from the server

Unplug the laptop from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

1. Remove the fiber cables that connect the following circuit packs in the PNs:
    - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
    - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Cutover to the server control

Because you do not reuse the PPN, you relocate the port network circuit packs to G650 Media Gateway.

When you relocate the circuit packs to the media gateway and you turn on the power, you want to cut over to have the new server control the existing PNs. The server can be an S8800 Server, Dell™ PowerEdge™ R610 Server or an HP ProLiant DL360 G7 Server. To cut over to the server, you must enable the IPSIs on the IP Server Interface (IPSI) System Parameters screen.

This stage affects service momentarily while the CSS comes up and the calls are load balanced across the IPSIs throughout the port networks.

Decommissioning the PPN

Because you do not reuse the PPN on the upgraded system, you must relocate the port network circuit packs to the new media gateway.

1. Turn off power to the PPN.
2. Remove all circuit packs from the PPN and place in antistatic bags. Set aside the port circuit packs for reuse.
3. Remove power supplies from the expansion control carriers.
4. Remove faceplate from the expansion control carriers.
5. Disconnect the following cables on the back of carrier A.
   - CURL
   - TDM/LAN
   - ICC-A and ICC-B
6. Remove the Current Limiter (CURL) unit from the back of the carrier. You can reuse the CURL.
7. Remove all carrier grounds.
8. Remove the expansion control carriers from the cabinet.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   ⚠ **Caution:**

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.
2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

Note:

You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or the customer wants to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
    - CURL - you cannot reuse this cable.
    - TDM/LAN - you can reuse this cable.
    - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on the first S8800 Server

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Verifying the Communication Manager operation

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:

   i. Click **Change**.
   ii. On the Change Current Schedule Web page, click **Change Schedule**

- To remove the schedule backup, click **Remove**.

  The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Postupgrade tasks on the second S8800 Server

Connecting the server to network

At this point, the service outage occurs.

1. Disconnect the LAN cable from the original server.
2. Connect the LAN cable to the new server.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

Perform this procedure only if IPSIs are present on the server.

1. Under **IPSI Firmware Upgrades**, select IPSI Version.
2. Under **Query Type**, select Query All and click **View** to verify the connectivity to all IPSIs.

Releasing the server

1. Under **Server**, select **Busy-Out/Release Server**.
2. On the Busy-Out/Release Server window, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay

- **Processes**: okay

3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the status for all operations is `UP STANDBY`.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Interchanging servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

1. Under **Server**, click **Interchange Servers**.
2. Click **Interchange**.
   The roles of the active and standby servers changes.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Chapter 6: Upgrading to embedded main template

Upgrading DEFINITY SI or CSI Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the following DEFINITY Servers to Communication Manager Release 6.0.1 on S8300D Server running System Platform and the embedded main template.

- DEFINITY SI Server in a SCC1 or an MCC1
- DEFINITY CSI Server in a CMC

In this procedure:

- You discard all the circuit packs and the cabinet.
- You install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring Communication Manager Release 6.0.1 on S8300D Server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.0.1.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.

- Decommissioning the cabinets.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license file for Communication Manager Release 6.0.1. This upgrade affects the service.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D Server.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Preupgrade administration

Connecting to the processor

Prerequisites

Cross-over cable.

1. Connect your Services laptop directly to the processor to access the cabinet.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.

2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Upgrade tasks

Inserting the S8300D Server in the branch gateway

Prerequisites

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

⚠ **Electrostatic alert:**

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.

   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:
You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

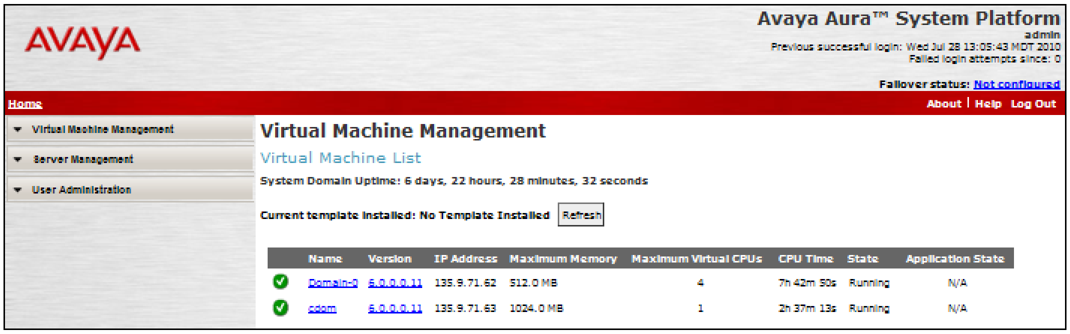
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**

- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the translations

Prerequisites

Log in to System Management Interface.

Use this procedure to restore translations only on the main server. When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

1. Under **Administration**, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**

- If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
- If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:

If the server is not connected to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the file to restore, for example, *_cmserver1_*.xln.

Important:

Do not restore a file with a name that starts with a "os_" or "full_". Restore only the files with the extension .xln.

6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the Restore status.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter y to configure basic gateway connectivity.
4. Configure the following parameters:

- VLAN number
- IP address and subnet mask for the primary management interface

  Note:

  The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
- IP address for the default gateway (router)
- Up to four IP addresses to specify the Media Gateway Controllers
- Hostname for the branch gateway

The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.

5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

Prerequisites

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Enter `add media-gateway <number>`, where <*number*> is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:
   - Enter `show system`.

- Note the serial number of the branch gateway.

  The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.

4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
   a. Select **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I’m using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.

The system displays the Messaging Administration screen.

3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.
   You can select four files at a time from the language CD that you want to copy to the server.

6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

    The default is **none**.

Removing fiber-related administration

Prerequisites

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Disconnecting from the server

Unplug the laptop from the services port.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

1. Remove the fiber cables that connect the following circuit packs in the PNs:
    - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
    - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Decommissioning the cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   ⚠ **Caution:**

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.

2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

   Note:

   You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or the customer wants to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
   - CURL - you cannot reuse this cable.
   - TDM/LAN - you can reuse this cable.
   - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.

9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on S8300D Server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:

- **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

> **Note:**
> Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Perform the procedures related to Communication Manager Messaging only if Communication Manager Messaging is enabled on this server.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.

3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300A Server to S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 1.x, 2.0, or 2.0.1 on an S8300A Server to Release 6.0.1 on an S8300D Server.

In this procedure, you replace the S8300A Server with an S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Upgrading Communication Manager Release 1.x, 2.0, or 2.0.1 on S8300A Server to Release 4.0.5 or Release 5.2.1 on S8300D Server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.0.1.
- Replacing the S8300A Server with an S8300D Server in the G700 Branch Gateway.

- Installing System Platform and embedded main template on S8300D Server.
- Restoring the data set that was created while on Release 4.0.5 or Release 5.2.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Checking the availability of the FTP, SFTP, or SCP server

Prerequisites

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP (for release 1.x, 2.0 or 2.0.1, the system supports only FTP) server over the customer LAN. You require a current version of the system data to restore the system configuration after you complete the upgrade.

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Preupgrade tasks on the S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

      If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.

2. Verify that the **Reports as:** field displays one of the following release numbers:

   - `R011x.02.0.110.4` for release 1.2
   - `R011x.03.2.536.1` for release 1.3.2
   - `R012x.00.0.219.0` for release 2.0
   - `R012x.00.1.221.1` for release 2.0.1

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Server Configuration**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.
      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Print or copy the information from the following screens:
   - **Set Identities**
   - **Configure Interfaces**

- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**

7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
    - **Alarms** > **SNMP Agents**
    - **Alarms** > **SNMP Traps**
    - **Server** > **Server Date/Time**
    - **Security** > **Server Access**
    - **Miscellaneous** > **CM Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

    c. Enter `almsnmpconf` and record the output.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Prerequisites

If you are using Telnet, enable the Telnet service for Communication Manager.

If Telnet is disabled, use SSH to access the SAT.

Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging on to the server with a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity. This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files to the FTP server.

Backing up the files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
    - **Avaya Call Processing (ACP) Translations**
    - **Server and System Files**
    - **Security Files**
    - **Communication Manager Messaging (CMM)**

      Select **Translations, Names, and Messages**.
3. Under **Backup Method**, select **Network Device**.
4. In the **Method** field, select one of the `FTP`, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Using the steps described in this section, you can download the following files:

- The latest available service pack for Communication Manager Release 4.0.5 or Release 5.2.1
- The RFA license for Communication Manager Release 4.0.5 or Release 5.2.1
- Avaya authentication file for Communication Manager Release 4.0.5 or Release 5.2.1
- Preupgrade service pack to upgrade from Communication Manager Release 4.0.5 or Release 5.2.1
- One of the following backup sets:
  - The three-part backup, `os_*.tar.gz`, `security_*.tar.gz`, and `xln_*.tar.gz`
  - Full backup, `full_*.tar.gz`

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Service pack for the current software version

You must obtain and activate the latest available service pack for the currently running Communication Manager software version before you proceed with the next upgrade steps. Depending on the release, use one of the following procedures to install the service pack.

Installing the preupgrade service pack on a server running release earlier than 2.0

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. Enter `cd /var/home/ftp` and press `Enter` to access the ftp directory.
5. At the prompt, enter `ls -ltr` and press `Enter`.

   The system displays a list of files in the `ftp` directory.
6. Verify that the directory contains the `*.tar.gz` file you have uploaded.
7. Enter `sudo patch_install patch.tar.gz`.

   Here, *patch* is the release or issue number of the service pack file. For example, `03.1.526.5-1003.tar.gz`.
8. Enter `patch_show` and press `Enter` to list the files to verify that the new software file is installed.
9. Enter `sudo patch_apply patch` and press `Enter`.

   Here, *patch* is the release or issue number of the service pack file. For example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.

   The server stops all processes. The server may also go through a software *reset system 4*. The reset process takes about 1–2 minutes and more than 2 minutes if messaging is enabled. Wait until the restart or reset process is complete and enter additional commands.
10. Enter `patch_show again` and press `Enter` to list files to verify the new software file was applied.
11. Enter `statapp -c` to view the status of the processes.

    Make sure that all processes except dupmgr are `UP`. Communication Manager must display `65/65 UP` or, if Communication Manager Messaging is installed, must display `67/67 UP`. To stop the continual refresh of the statapp command, enter `Ctrl-C`.

    Note:

    The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number.

For example, the numbers 64/65 UP indicate that a process did not come up and should be investigated before proceeding.

12. Close the Telnet session.

Installing the preupgrade service pack on a server running release 2.0

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

   If the media server reboots, it may display `/opt/ecs/sbin/drestart 2 4 command failed` message. Ignore this message. Wait until the restart or reset completes before entering additional commands. The media server displays a message that the service pack is applied.
8. Enter `update_show` and press `Enter` to list Communication Manager files and verify that the new service pack file is activated.
9. Close the Telnet session.

Backing up the files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**

- **Server and System Files**
- **Security Files**
- **Communication Manager Messaging (CMM)**

   Select **Translations, Names, and Messages**.

3. Under **Backup Method**, select **Network Device**.
4. In the **Method** field, select one of the `FTP`, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **Start Backup**.
6. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `full_cmserver_172731_20100516.tar.gz` or the three-set backup `os_cmserver_123456_20100725.tar.gz`, `security_cmserver_123456_20100725.tar.gz`, and `xln_cmserver_123456_20100725.tar.gz`.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341 to record the information.

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
   - Server IP address
   - Gateway IP address
   - Subnet mask
   - Integrated Messaging IP address, if configured.
6. Click **Close**.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.

The system displays the Backup History page and a list of recent backups.

11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
   - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Upgrade tasks on the S8300D (Release 4.0.1 or 5.2.1) Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

Installing Communication Manager

Prerequisites

CD/DVD for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

1. On your laptop, click **Start** > **Run** to open the Run dialog box.
2. Enter `ping -t 192.11.13.6` and press `Enter`. Wait for the reply.

   The installation script looks for the software CD in the CD/DVD drive connected to the USB port. If the CD/DVD drive was not attached to a USB port when the server booted, the system displays the `Request Timed Out` message on the screen. You must then unseat and reseat the S8300D server in its slot.

   Tip:

   To navigate the installation screens, use the arrow keys to move to an option and press the space bar to select the option. Press `Enter`.
3. Select **Install** and press `Enter`.
4. On the Select Release Version screen, select the appropriate release version and click **OK**.

   The system displays the Run Communication Manager Messaging Installation screen. Install Communication Manager Messaging only if messaging was enabled on the S8300A.
5. Complete one of the following:
   - To install Communication Manager Messaging concurrently with Communication Manager, select **Yes**.
   - To skip the installation of Communication Manager Messaging, select **No**.

   The installation process:
   - Partitions and reformats the hard drive and internal compact flash of the server.
   - Installs the Linux operating system.

- Installs Communication Manager and reports the progress.
- If you select **Yes**, installs Communication Manager Messaging.

The installation process takes about 30 minutes. When the server is ready to reboot, the DVD drive door opens and a reminder to check the Avaya Support Site at http://support.avaya.com for the latest software and firmware updates appears. Remove the DVD from the drive. The reboot takes about 5–8 minutes without Communication Manager Messaging and takes about 8–10 minutes with Communication Manager Messaging. The Telnet session ends automatically.

6. Click **Start** > **Run** to open the Run dialog box.
7. Enter `ping -t 192.11.13.6` and press `Enter`.
8. Wait for the reply from the server to ensure connectivity to it.
9. For the remaining steps on installing Communication Manager and co-resident applications, see *Installing and Configuring the Avaya S8300 Server* (555-234-100).

Checking the reboot progress

1. On the laptop, click **Start** > **Run**.
2. Enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter` to clear the ARP cache.
   - The system displays the command line prompt if the cache is cleared.
   - The system displays the message, `The specified entry was not found`, if the specified IP address does not contain an entry in the ARP cache.
4. Enter `ping -t 192.11.13.6` to access the media server.

   The -t causes the ping to repeat. When you get a response (in about 3 minutes), wait an additional 30 seconds before you access the Web interface.
5. Enter `Ctrl+c` to stop the ping.
6. Close the MS-DOS window.

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

The system displays the Software Version page.

2. Verify that the **CM Reports as:** field displays one of the following:
    - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

      This means that Communication Manager Release 4.0.5 is running on the server.
    - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

      This means that Communication Manager Release 5.2.1 is running on the server.

Setting the time, date, and time zone

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Server Date/Time**.
   The system displays the Server Date/Time page.
2. Set the server time within five (5) minutes of the Network Timer Server (NTS) time, date and time zone so that synchronization can occur.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Prerequisites

- Log on to System Management Interface.
- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure if the server is running Communication Manager release 4.0 or later.

Important:
You must perform this task before you proceed with the next upgrade procedures.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **update ID** and click **Activate**.

        The system displays the status as the update progresses. The system automatically reboots, if required.
     2. Click **Yes**.
3. Click **Continue**.

   Note:
   Do not install the preupgrade service pack until instructed.

Configuring network parameters

Prerequisites

- Obtain the host name, subnet mask, and IP addresses of the server and default gateway.
- Log on to System Management Interface.

You can configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Under **Installation**, click **Configure Server**.

   The system opens the Configure Server wizard.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the **Configure Individual IP Services** list.
5. On the Set Identities page, enter the host name of the server.
6. Click **Continue**.
7. On the Configure Interfaces page, enter the IP address for the server and gateway and the subnet mask. If Communication Manager Messaging is installed, enter the IP address.

   If these fields are already filled in, overwrite them with the correct information. Leave the **Integrated Message** field blank.
8. Click **Change** to update the system files.

   If the system displays the `Action Cancelled` message before it displays the `Success` message, refresh the screen and click **Change** again.

   When the configuration change is complete, the system displays the `Successfully configured ethernet interfaces` message.

Restoring backup data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. Select **Network Device**.

3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
5. Click **View**.

    The system displays the View/Restore Data Results page.
6. Select the backup name and click **Restore**.
7. To monitor the restore progress, select **Data Backup/ Restore** > **Restore History**.

    The system displays the Restore History page.
8. Select the backup file that you want to monitor and click **Check Status**.

    The system displays the Restore History Results page.
9. Click **Refresh** periodically until the message indicates that the restore is successful.

    This refresh process takes about 5 minutes.
10. Repeat Step 1 through Step 9 to restore:
    - Security data set, if not performed in Step 6
    - Communication Manager translations data
    - Messaging application data in the `audix-tr-name-msg` file
    - Messaging application announcements in the `audix-ann` file

Creating a super-user login

Note:

The craft level login can create a super-user login.

1. Ask a customer representative for a login name and password that the customer would like for the super-user login. If you are a Business Partner, you can also add the dadmin login.

Note:

Ensure that the customer can change this login, its password, or its permissions.

2. Log on to the System Management Interface and select **Administration > Server (Maintenance) > Administrator Accounts.**
   The system displays the Administrator Accounts page.
3. Select **Add Login**.
4. Select **Privileged Administrator** and click **Submit**.
   The system displays the Administrator Logins -- Add Login: Privileged Administrator page.
5. Type a login name for the account in the **Login name** field.
6. Verify the following:
   - `susers` appears in the `Primary group` field.
   - `prof18` appears in the `Additional groups (profile)` field. prof18 is the code for the customer superuser.
   - `/bin/bash` appears in the `Linux shell` field.
   - `/var/home/login` name appears in the `Home directory` field, where login name is the name you entered in step 5.
7. Skip the fields **Lock this account** and **Date on which account is disabled-blank to ignore**.
8. From the **Select type of authentication** option, select **password**.

   Note:

   Do not lock the account or set the password to be disabled.
9. Enter the password in the **Enter password or key** field and the **Re-enter password or key** field.
10. In the section Force password/key change on next login select **no**.
11. Click **Submit**.
    The system informs you the login is added successfully.

Checking for the Communication Manager Messaging IP address

1. Under **Switch Link Administration**, click **Switch Link Admin**.
2. Under **Link Addresses**, in the **Switch** field, verify the IP address of Communication Manager Messaging.

Installing the CM license and authentication files

⚠ **Caution:**

A super-user login, dadmin, or other customer super-user login must exist before you install an authentication file. See Creating a super-user login on page 111.

1. Log on to the System Management Interface and select **Administration > Server (Maintenance) > License File**.
   The system displays the License File page.
2. Select **Install the license file I previously downloaded** (radio button) and click **Submit**.
   The system displays a message indicating that the license is installed successfully.
3. On the System Management Interface, select **Administration > Server (Maintenance) > Authentication File**.
   The system displays the Authentication File page.
4. Select **Install the Authentication file I previously downloaded** (radio button) and click **Install**.
   The system displays a message indicating that the authentication file is installed successfully.
5. Verify the license and authentication file installation by running the `statuslicense -v` command from the server command line:
   - The `License Mode` should be `Normal`.
   - The report should list a `License Serial Number`.

Rebooting the server

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Shutdown Server**.
2. Select the following check boxes:
   - **Restart server after shutdown**
   - **Shutdown even if this is the active server**
3. Click **Shutdown**.
   The system displays the `A server shutdown has been requested` message.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

      The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

Prerequisites

Log on the Maintenance Web page.

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
5. Click **OK**.
6. When the **OK to Remove LED** on the faceplate of the server is steady, it is safe to remove the server.

Upgrade tasks on the S8300D (Release 6.0.1) Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:

If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Communication Manager Messaging file.

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

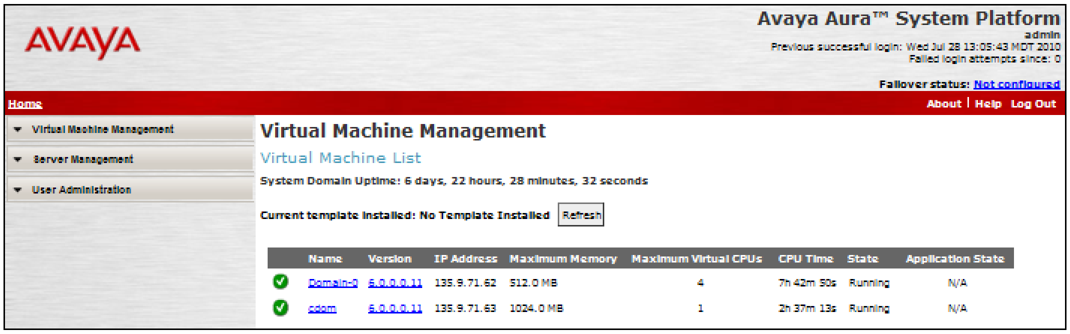
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Avaya Aura™ System Platform

admin

Previous successful login: Wed Jul 28 13:05:43 MDT 2010

Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

Note:

If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:

- Click **Network Device** and complete the following fields:
    - **Method**
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory** or **Field Path**
        - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
        - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
- Click **Local Directory** and provide the path to the backup file on your local directory.

> **Important:**
> If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
    The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
    - File(s) to download from the machine I'm using to connect to the server.
    - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the RFU.

- Enter the URL to download the RFU and enter the host name and domain name of the proxy server.

5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
4. Click **View**.

5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
   This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.
   You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.

   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

5. Enter `change signaling-group <num>`.

   a. In the **Far-end Node Name** field, enter `msgserver`.

   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.

6. Enter `release signaling-group <num>`.

7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.

8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

Alternatively, you can reboot the server using System Management Interface. To do that:

a. Under **Server**, click **Shutdown Server**.

b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
    - To change the schedule backup:
        i. Click **Change**.
        ii. On the Change Current Schedule Web page, click **Change Schedule**
    - To remove the schedule backup, click **Remove**.

      The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

> **Important:**
> The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

> **Note:**
> Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.0.1 for existing Communication Manager on an S8300B or S8300C Server.

In this procedure, you replace the S8300B or S8300C Server by an S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

For S8300A server, on Communication Manager release earlier than 5.2.1, perform the upgrade as instructed in the section “Upgrading the Avaya S8300A server to embedded main on S8300D Server”.

Upgrade paths

You can upgrade the following S8300 servers running a supported release of Communication Manager to S8300D server:

- S8300C as main server
- S8300B as main server

Required upgrade sequence

Perform the upgrades in the following sequence:

- The branch gateway firmware
- The media module firmware
- Communication Manager on the survivable remote server
- Communication Manager on the main server

Upgrade tasks on the S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

This means that Communication Manager Release 4.0.5 is running on the server.

- `R015x.02.1.016.4` for Communication Manager Release 5.2.1

  This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.
      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.

c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

d. Click **Save**.

6. Click **Administration** > **Server (Maintenance)**.

7. Print or copy the information from the following screens:

   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

   If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.

9. On the command line prompt, perform the following:

   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

   b. Enter `productid` and copy the value for product ID.

Checking the availability of the FTP, SFTP, or SCP server

Prerequisites

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP (for release 1.x, 2.0 or 2.0.1, the system supports only FTP) server over the customer LAN. You require a current version of the system data to restore the system configuration after you complete the upgrade.

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.

- If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.

3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, Select **Full Backup** (release-dependent).

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.

ii. Wait until the system displays the message, `... unpacked successfully`.

- If the status of the update file you want to activate is unpacked:

   i. Select the **Update ID** and click **Activate**.

   ii. The system displays the status as the update progresses. The system automatically reboots, if required.

   iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.
   If you find any announcement sets other than the following, proceed with Step 3:
   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**
    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
    - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

    The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.

4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    > ⚠ **Caution:**
    >
    > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the devices from the server

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the server

Prerequisites

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.
- Connect the USB CD/DVD drive.
- Insert the System Platform media.

⚠ **Caution:**

Ensure that you wear a properly grounded ESD wrist strap when handling the server. Place all components on a grounded, static-free surface when working on them.

1. Loosen the two thumb screws on the faceplate of the server.
2. When removing the server, remove the LED panel (above slot V1) (G700 only) or the space bar (G250, G350 and G450) with the server.
    - For G700, disengage the LED panel and the server, and remove them together from the branch gateway.
    - For G250, G350 or G450, remove the space bar and the server.
    - For G430, remove the server from the branch gateway.
3. Perform one of the following:
    - For G700, partially reinsert the LED panel (above slot V1) and the new S8300D server (slot V1). Leave them extended from the branch gateway by about 1 inch (2.5 cm).

      Do not seat these circuit packs now.

- For G250, G350, G430 and G450, partially reinsert the new S8300D Server (slot V1). Leave the server extended from the branch gateway by about 1 inch (2.5 cm). Do not seat this circuit pack now.

4. With the S8300D in slot V1 still extended, by about 1 inch (2.5 cm), connect the USB CD/DVD drive to any one of the USB ports.
5. When you are ready to start installing System Platform, seat the S8300D Server (for G700, also seat the LED panel) into the branch gateway by gently pressing it until the faceplate is aligned with the face of the branch gateway.
   a. Insert the System Platform media into the USB CD/DVD drive within by about 30 seconds of seating the S8300D Server.
   b. If the media is not present in the CD/DVD drive or if the USB CD/DVD drive is not connected to the server at the time of boot, you must repeat the Step 5.

      Alternatively, reboot the server by powering up and powering down the branch gateway.

      When the server starts to boot, it looks for the software on the DVD/CD-ROM. The Alarm LED of the S8300 Server is steady as it is starting. The Alarm LED starts flashing when the S8300 Server is ready to load software.
6. Secure the faceplate of the S8300D server with the thumb screws. Tighten the thumb screws with a screw driver. For G250, G350, and G450, secure the space bar above slot V1
7. Reconnect the laptop to the services port of the new S8300D server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:

If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Communication Manager Messaging file.

Note:

You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

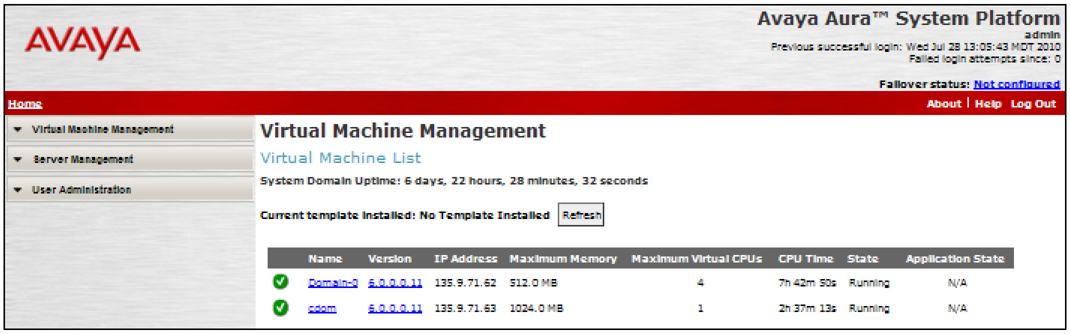
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Fallover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:
You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:
    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
    The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:
   Communication Manager Messaging processes are stopped during RFU installation.

If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.

   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
    a. In the **Name** field, enter `tmp`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
    This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
    a. Record the value of the **Far-end Node Name** field.
    You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
    b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
    a. In the **Name** field, enter `msgserver`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
    a. In the **Far-end Node Name** field, enter `msgserver`.
    b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.
    Remove the entries from the **Name** and **IP Address** fields and submit the form.
    This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.

5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.

The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:
     1. Click **Change**.
     2. On the Change Current Schedule Web page, click **Change Schedule**
   - To remove the schedule backup, click **Remove**.

     The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:

   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.

5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8400 Server running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.0.1 on S8300D Server.

In this procedure:

- You discard:
  - All circuit packs
  - The G600, G650 Media Gateway or the CMC cabinet
- You install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Restoring the data set on Communication Manager Release 6.0.1.
- Restoring Communication Manager Messaging data set.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1.

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.0.1. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D Server.

Preupgrade tasks on the S8400 Server

Connecting to the server

Prerequisites

A CAT5 cross-over cable to connect your services laptop to the server.

1. Plug one end of the CAT5 cross-over cable into the services access port on the server faceplate.
2. Plug the other end of the cross-over cable into the services laptop.
3. Start a SAT session.
4. Log in as `craft`.

Accessing System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**

Starting a SAT session

Prerequisites

If you are using Telnet, enable the Telnet service for Communication Manager.

If Telnet is disabled, use SSH to access the SAT.

Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging on to the server with a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

You back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

If Communication Manager Messaging is enabled on your system, back up the messaging data.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up the files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
    - **Avaya Call Processing (ACP) Translations**
    - **Server and System Files**
    - **Security Files**
    - **Communication Manager Messaging (CMM)**

        Select **Translations, Names, and Messages**.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   Caution:
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341 to record the information.

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
    - Server IP address
    - Gateway IP address
    - Subnet mask
    - Integrated Messaging IP address, if configured.
6. Click **Close**.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

    Note:

    Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

    You can select four files at a time.
5. Click **Download** to copy the files to the server.
    The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.

The system displays the Linux Migration - Backup Results dialog box.

4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > ⚠ **Caution:**
   >
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.

The system displays the Backup History page and a list of recent backups.

11. Select the backup from the list and click **Check Status**.

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

    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
    - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

    The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    Caution:
    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Prerequisites

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

⚠ **Electrostatic alert:**

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.

   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

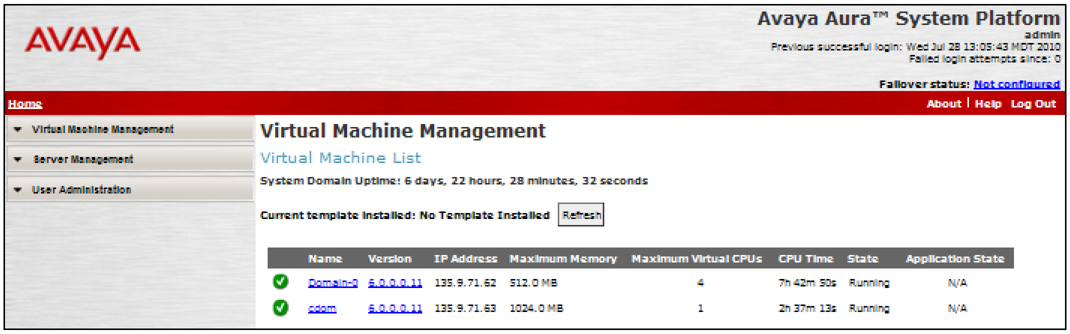
   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**

- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:
You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**

    - If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
    - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
  - Click **Local Directory** and provide the path to the backup file on your local directory.

  Important:

  If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
    - VLAN number
    - IP address and subnet mask for the primary management interface

      Note:
      The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
    - IP address for the default gateway (router)
    - Up to four IP addresses to specify the Media Gateway Controllers
    - Hostname for the branch gateway

    The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
    a. Enter `add mgc list` *`IP of CM procr / clan`*.
    b. Enter `copy running-config startup-config`.
    c. Enter `reset`.

Adding a branch gateway in Communication Manager

Prerequisites

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Enter `add media-gateway <number>`, where <*number*> is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:

   - Enter `show system`.
   - Note the serial number of the branch gateway.

     The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.
4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.
5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.
6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
   a. Select **Miscellaneous** > **Messaging Software**.
   The Messaging Software page displays `Internal messaging is disabled`.
   b. Click **Enable**.
   The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.

3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.

4. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.

- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.
      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

Note:

Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Completion tasks on the S8400 Server

Shutting down the server

1. Push and hold the **Shutdown** button on the faceplate of the server for more than 2 seconds.

The **OK to Remove LED** in green flashes to indicate that shutdown is in progress.

2. When the green **OK to Remove LED** is steady, unlatch the circuit pack, slide it out of its slot.
3. Leave the compact flash card with translations in the slot.
4. Leave cable adapter of the server attached at the rear of the carrier and its cable connections in place during the entire replacement procedure.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Turning off the power to the port network

1. From the bash prompt on the services laptop, enter `shutdown system` and press `Enter`.

   This shuts down the server gracefully.
2. Wait until the **Shutdown Complete** LED on the lower portion of the faceplate of the server is solid green.
3. Turn off the power to the media gateway for safety purpose.

   ⚠ **Danger:**

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the media gateway, pull the AC power cord from the back of the media gateway.
4. Unplug the power cord for safety purpose.

Upgrading S8500 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8500 main server running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.0.1 on S8300D Server.

In this procedure:

- You discard:
  - All port networks (CMCs, SCCs, MCCs or IP600)
  - All circuit packs and any gateways above 50
  - The S8500 Server and the G650 Media Gateway
- You install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Restoring the data set on Communication Manager Release 6.0.1.
- Restoring Communication Manager Messaging data set.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1.

You can upgrade Communication Manager running releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first, before you upgrade to Release 6.0.1. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D Server.

Preupgrade tasks on S8500 Server

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)

4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**

- **Set Identities**
- **Configure Interfaces**
- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging in from a laptop directly connected to the services port, perform one of the following:
    - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
    - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.
   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Checking clock synchronization

1. Type `status synchronization`.
2. Press **Enter** to verify that the clock synchronization is good.
3. Ensure that the **Switching Capabilities** field shows **enabled**.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
    - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
    - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

    For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations (main only)

The **`save translation`** command is dependent on the server role.

Perform one of the following steps:

- Enter `save translation` and `HELP`. If the system displays `[all or lsp]` or `[all or ess or lsp]`, enter `save translation all`.

- Enter `save translation` and `HELP`. If the system displays `[lsp or [ip address]]`, enter `save translation lsp`.
- Enter `save translation`.

Note:

If this operation fails, follow the escalation procedures before you continue with the next step.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

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

```
Backup successful
```

> ⚠ **Caution:**
> Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

     > **Note:**
     > For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:
     >
     > \- **Avaya Call Processing (ACP) Translations**
     >
     > \- **Server and System Files**
     >
     > \- **Security Files**

   - If Communication Manager Messaging is enabled:

     i. Select **Specify Data Sets**.

     ii. Select the following check boxes:

     - **Avaya Call Processing (ACP) Translations**

     - **Server and System Files**

     - **Security Files**

     - **Communication Manager Messaging (CMM)**

     Select **Translations, Names, and Messages**.

   iii. In the **Download size** field, enter the size of the backup .tar file.

        There could be more than one .tar file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**. Enter the host IP address.
    - **Directory**

    When the backup process is complete, the system saves the migration-60*.tar.gz file to the /var/home/ftp/pub location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.

4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
    - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

    The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

    There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**

8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Prerequisites

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

⚠ **Electrostatic alert:**

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides

6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:
   Media modules are restricted to certain slots.

9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.

11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

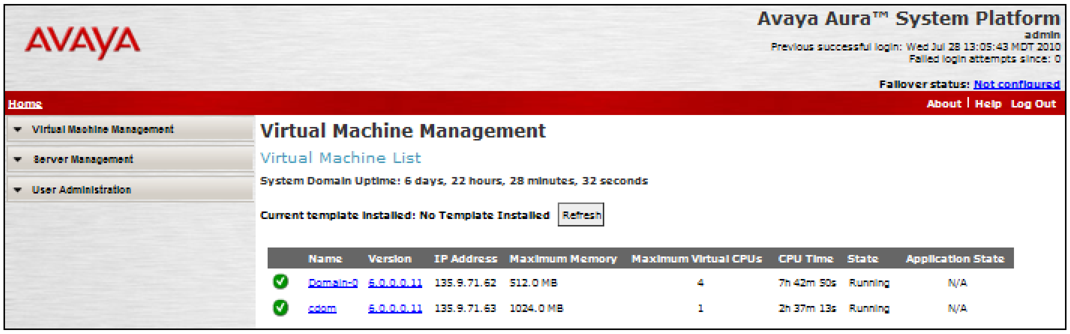
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two

ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:
     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**

- **Network Configuration**

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:
     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

Prerequisites

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Enter `add media-gateway <number>`, where <*number*> is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:

   - Enter `show system`.
   - Note the serial number of the branch gateway.

     The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.
4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.
5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.
6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect

- If the IP connection between the branch gateway and the S8300D Server is not established
- If the branch gateway is not registered with Communication Manager

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
       The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
       The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
    - File(s) to download from the machine I’m using to connect to the server.

- File(s) to download from the LAN using URL.

4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the RFU.
    - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.

5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   1. In the **Name** field, enter `tmp`.
   2. In the **IP Address** field, enter `<procr IP addr>` and submit the form. This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   1. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   2. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   1. In the **Name** field, enter `msgserver`.

   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.

5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

Alternatively, you can reboot the server using System Management Interface. To do that:

a. Under **Server**, click **Shutdown Server**.
b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Completion tasks on S8500 Server

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting from the server

Unplug the laptop from the services port.

Removing the server from the rack

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.

8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   > **Important:**
   > The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   > **Note:**
   > Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300D Server to S8300D Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 to Release 6.0.1 on an S8300D Server.

In this procedure, you reuse the existing S8300D Server and install System Platform and the embedded main template (CM_OnlyEmbed).

The embedded main template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

Communication Manager does not support upgrading SIP Enablement Services (SES) to Release 6.0.1.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

For S8300D Server on Communication Manager release earlier than 5.2.1, upgrade to Release 5.2.1 first before you upgrade it to Release 6.0.1. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**
    - **Set Identities**
    - **Configure Interfaces**
    - **Set DNS/DHCP**
    - **Set Static Routes**
    - **Configure Time Server**
    - **Server Access**
    - **Server Date/Time**

- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Verifying the current software release

1. Under **Server**, click **Software Version**.
   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
    - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
        - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
    - If you are logging in from a laptop directly connected to the services port, perform one of the following:
        - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
        - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message: `Backup successful`

   Caution:
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

Note:

For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

- **Avaya Call Processing (ACP) Translations**
- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:

  i. Select **Specify Data Sets**.

  ii. Select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
  - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.

  iii. In the **Download size** field, enter the size of the backup `.tar` file.

  There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.

   ii. Wait until the system displays the message, `... unpacked successfully`.

- If the status of the update file you want to activate is unpacked:
   i. Select the **Update ID** and click **Activate**.
   ii. The system displays the status as the update progresses. The system automatically reboots, if required.
   iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
3. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.
   If you find any announcement sets other than the following, proceed with Step 3:
   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
    - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.

4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    Caution:

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Verify if the **Restart server after shutdown** check box is selected.

Disconnecting the devices from server

Disconnect the USB CD/DVD reader from the server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:
  If you are upgrading a survivable remote server, do not install the Communication Manager license file.
- The Communication Manager Messaging file.

  Note:
  You need the Communication Manager Messaging license file only if Communication Manager Messaging was enabled on the existing server.
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

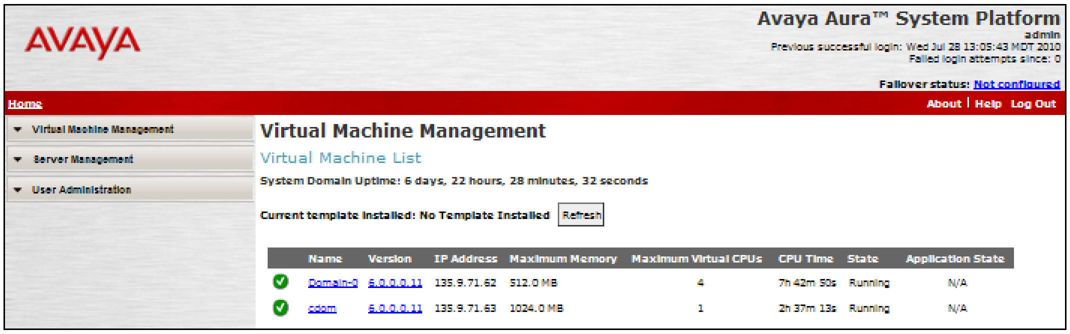
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing service pack

Prerequisites

- Copy the latest service packs from the Avaya Support Site to the Services laptop.
- Log on to the System Platform Web console.

Use this procedure to install the service packs for System Platform and Communication Manager.

Important:
You must perform this task before you proceed to the next upgrade procedures.

1. Under **Server Management**, click **Patch Management** > **Download/Upload**.
2. In the **Choose Media** field, select the media where the service packs are located.
3. If the file is located on the computer, click **Add** and browse to the location of the file.
4. Click **Upload**.
5. Click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

Note:

If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.

    - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
  - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.

3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:

a. Select **Miscellaneous** > **Messaging Software**.

   The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

   The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   > **Important:**
   >
   > Communication Manager Messaging processes are stopped during RFU installation.
   >
   > If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.
   >
   > Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

You can select four files at a time from the language CD that you want to copy to the server.

6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**

- **Directory**

5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   1. In the **Name** field, enter `tmp`.
   2. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   1. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   2. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   1. In the **Name** field, enter `msgserver`.
   2. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   1. In the **Far-end Node Name** field, enter `msgserver`.
   2. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
    - **Server Hardware**: okay
    - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Verifying destination for scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

You must change or remove the scheduled backups that have USB flash card as the destination.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup to change or remove and complete one of the following:
   - To change the schedule backup:

   i. Click **Change**.
   ii. On the Change Current Schedule Web page, click **Change Schedule**

- To remove the schedule backup, click **Remove**.

  The system removes the backup schedule you deleted from the list.

Resubmitting the scheduled backups

Communication Manager Release 6.x does not support backing up to a flashcard.

Resubmit all schedule backups to make them compatible with Release 6.x.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Chapter 7: Upgrading to embedded survivable remote template

Upgrading DEFINITY SI or CSI Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the following DEFINITY Server to Communication Manager Release 6.0.1 on S8300D Server running System Platform and the embedded survivable remote template.

- DEFINITY SI Server in a SCC1 or an MCC1
- DEFINITY CSI Server in a CMC

In this procedure:

- You discard all the circuit packs and the cabinet.
- You install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded main template (CM_SurvRemoteEmbed).

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring Communication Manager Release 6.0.1 on S8300D Server.
- Decommissioning the cabinets.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

You require a new authentication file for Communication Manager Release 6.0.1 configured as survivable remote server.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.

✔	Task	Description
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D Server.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Preupgrade administration

Connecting to the processor

Prerequisites

Cross-over cable.

1. Connect your Services laptop directly to the processor to access the cabinet.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.

3. Record the equipment that is busied out.

Upgrade tasks

Inserting the S8300D Server in the branch gateway

Prerequisites

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

⚠ **Electrostatic alert:**

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.
10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.
11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

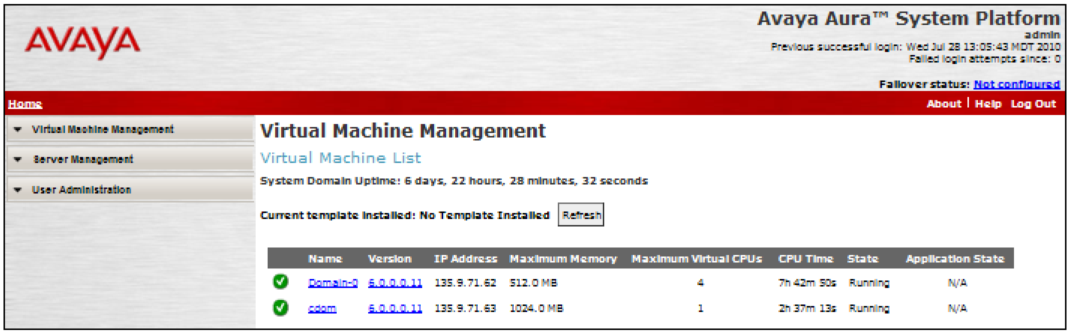
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.


AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.

3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
    - VLAN number
    - IP address and subnet mask for the primary management interface

      Note:
      The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
    - IP address for the default gateway (router)
    - Up to four IP addresses to specify the Media Gateway Controllers
    - Hostname for the branch gateway

    The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
    a. Enter `add mgc list` *`IP of CM procr / clan`*.
    b. Enter `copy running-config startup-config`.
    c. Enter `reset`.

Adding a branch gateway in Communication Manager

Prerequisites

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Enter `add media-gateway <number>`, where <*number*> is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

To obtain the serial number of the branch gateway, on the command prompt of the gateway:

- Enter `show system`.
- Note the serial number of the branch gateway.

  The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.

4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.

5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.

6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:

- If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Removing fiber-related administration

Prerequisites

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Removing the processor port network control cabinet

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

1. Label both ends of all the cables that you will remove from all the cabinets. You will reuse these cables.

   ⚠ **Caution:**

   The system drops all active calls that are processed through this PN when you turn off the cabinet stack. All trunks and lines within this cabinet stack remains out-of-service until the cabinet stack is turned on and the server controls the PN.

   Note:

   If the system is equipped with power failure transfer (PFT) units that use ground start trunks, you must install a temporary ground wire to the PFT units. This ground wire allows units to operate correctly when the cabinet is turned off. The AUX cable that usually supplies the ground is disconnected.
2. Connect a 10 AWG (#25) (2.6 mm^2) wire to pin 49 of the connecting block or to pin 49 of the cable access panel (CAP) on the power-failure transfer panel.
3. Route the opposite end of the wire to an approved ground and connect.

Note:

You can cut over and have the server control the other PNs at this time. Cutover at this time if you are not installing IPSI(s) in the PPN or the customer wants to minimize out-of-service time.

4. Turn off the cabinets in the SCC1 stack.
5. Remove all circuit packs from the cabinets and place the circuit packs in an antistatic carrier or bag.
6. Disconnect the cables on the front of the cabinets.
7. Disconnect the following cables on the back of the cabinets.
    - CURL - you cannot reuse this cable.
    - TDM/LAN - you can reuse this cable.
    - ICC-A, ICC-B - you can reuse this cable.
8. Remove all cabinet grounds.
9. Remove the top cabinet.
10. If this system has a duplicated bearer network, remove the subsequent cabinets, including control cabinet A and control cabinet B.

Postupgrade tasks on S8300D Server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.

2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.

2. Depending on the server configuration, choose one of the following:

   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

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.

4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

   Note:

   Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Removing the cabinet and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the cabinet from the rack.
2. Discard all the circuit packs you removed from the cabinet.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300A server to S8300D server

Introduction

This section describes the procedure to upgrade Communication Manager Release 1.x, 2.0 or 2.0.1 on an S8300A Server to Release 6.0.1 on an S8300D Server.

The procedure requires you to replace the S8300A Server configured as survivable remote processor, formerly local survivable processor (LSP) with an S8300D Server running System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

The upgrade procedure involves:

- Recording the configuration information from the existing S8300A Server in the upgrade worksheet.
- Upgrading the branch gateway firmware to make it compatible with Release 6.0.1.
- Replacing the S8300A Server with an S8300D Server in the G700 Branch Gateway.
- Installing System Platform and the embedded survivable remote template on the S8300D Server.
- Configuring Communication Manager to work as survivable remote.

The upgrade procedure synchronizes translations and user accounts from the main Communication Manager server to the survivable remote processor. You require a new authentication file for Communication Manager release 6.0.1 configured as survivable remote server.

Onsite preparation

USB DVD/CD-ROM drives

To upgrade an S8300 Server to an S8300D Server, you must install System Platform software and Communication Manager software on the new server. You need a USB DVD/CD-ROM drive at the site to do this.

S8300 server supports Avaya approved Panasonic Digistor 73082 or 73322 external CD/DVD-ROM drives.

- The switch must be set to ON.
- The Panasonic Digistor CD/DVD-ROM drives draw more power than the USB port can supply. Therefore, instead of AC power, the Panasonic Digistor drives use a Lithium ION battery to supply the additional power. If the Lithium ION battery is depleted, the system displays a red LED and the message `failed to mount CD-ROM`. You can charge the Lithium ION battery by plugging the CD-ROM drive into a USB port for approximately 30 minutes. The Lithium ION battery charges faster if the switch is set to OFF.

Note:

The Lithium ION battery supplies the extra power only to Panasonic Disgistor CD/DVD-ROM drives.

Checking the availability of the FTP, SFTP, or SCP server

Prerequisites

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP (for release 1.x, 2.0 or 2.0.1, the system supports only FTP) server over the customer LAN. You require a current version of the system data to restore the system configuration after you complete the upgrade.

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

On the S8300A server

Clearing the ARP cache on the laptop computer

You may have to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address depending on the operating system running on your laptop computer. If you fail to clear the cache, your computer does not connect to the server.

1. To open the Run dialog box, click **Start** > **Run**
2. To open an MS-DOS command line window, enter `command` and press `Enter`.
3. Enter `arp -d 192.11.13.6` and press `Enter`.

   This command produces one of the following responses:

   - The command line prompt displays when the cache is cleared.
   - The message `The specified entry was not found` appears when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

1. Perform one of the following:
   - If onsite, connect to the services port labeled as *2* on the back of the media server.
   - If offsite, log on to the media server using the unique IP address of the media server.
2. Launch the Web browser.
3. Enter `192.11.13.6` in the **Address** field.
4. Log on as `craft` or `dadmin`.
5. Click **Launch Maintenance Web Interface**.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **Reports as:** field displays one of the following release numbers:
   - `R011x.02.0.110.4` for release 1.2
   - `R011x.03.2.536.1` for release 1.3.2
   - `R012x.00.0.219.0` for release 2.0
   - `R012x.00.1.221.1` for release 2.0.1

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

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

3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.

       The configuration screen appears in your application window.

    b. Click **File** and select **Save As**.

    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.

    d. Click **Save**.
6. Print or copy the information from the following screens:
    - **Set Identities**
    - **Configure Interfaces**
    - **Set DNS/DHCP**
    - **Set Static Routes**
    - **Configure Time Server**
7. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
8. Click **Administration** > **Server (Maintenance)**.
9. Print or copy the information from the following screens:
    - **Alarms** > **SNMP Agents**
    - **Alarms** > **SNMP Traps**
    - **Server** > **Server Date/Time**
    - **Security** > **Server Access**
    - **Miscellaneous** > **CM Phone Message File**

      If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
10. After you copy or print the screens, click **Cancel**. *Do not* click **Submit**.
11. On the command line prompt, perform the following:
    a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).

    b. Enter `productid` and copy the value for product ID.

    c. Enter `almsnmpconf` and record the output.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341 to record the information.

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
    - Server IP address
    - Gateway IP address
    - Subnet mask
    - Integrated Messaging IP address, if configured.
6. Click **Close**.

Recording the scheduled backups

Record the backup scheduled for the existing server. You must submit the scheduled backups after the upgrade.

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. Record the details of any backup schedules.

   You will submit these scheduled backups after the upgrade on the new server running Communication Manager Release 6.0.x.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity. This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files to the FTP server.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - Select **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     i. Select **Specify Data Sets**.
     ii. Select the check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
3. In the **Download size** field, enter the size of the backup `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.

The system displays the Backup History page and a list of recent backups.

8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   > **Caution:**
   > Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

Prerequisites

Log on the Maintenance Web page.

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
5. Click **OK**.
6. When the **OK to Remove LED** on the faceplate of the server is steady, it is safe to remove the server.

Disconnecting the devices from the server

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the S8300A Server

Prerequisites

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.

⚠ **Warning:**

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Loosen the two thumb screws on the faceplate of the server.
2. Disengage the LED panel and the server, and remove them together from the gateway.
3. Partially reinsert the LED panel (above slot V1) and the new S8300D Server (slot V1). Leave them extended from the gateway by about 1 inch (2.5 cm).

   Do not seat these circuit packs now.
4. With the S8300D Server in slot V1 still extended, connect the USB CD/DVD drive to any one of the USB ports.
5. When you are ready to start installing System Platform, seat the S8300D Server and the LED panel into the gateway by gently pressing it until the faceplate is aligned with the face of the gateway.
6. Insert the System Platform media into the USB CD/DVD drive within by about 30 seconds of seating the S8300D Server.

   Note:

   If the media is not present in the CD/DVD drive or if the USB CD/DVD drive is not connected to the server at the time of boot, repeat Step 5.

   Alternatively, reboot the S8300D Server by powering up and powering down the gateway.

   When the server starts to boot, it looks for the software on the DVD/CD-ROM. The Alarm LED of the S8300D Server is steady as it is starting. The Alarm LED starts flashing when the S8300D Server is ready to load software.
7. Secure the faceplate of the S8300D Server with the thumb screws. Tighten the thumb screws with a screw driver.
8. Reconnect the laptop to the services port of the S8300D Server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:

  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

   c. In the command line, type **`service_port_access enable`** and press **Enter**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

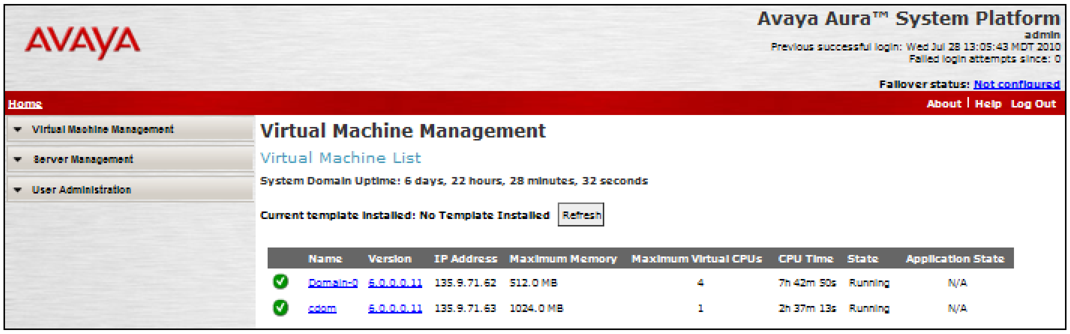
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**

- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Configuring the alarming information

Prerequisites

Log on to System Management Interface.

Configure the information provided in the worksheet available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431).

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Submitting the scheduled backups

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. On the Schedule Backup Web page, select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.

3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.

6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8300 Server to S8300D Server

Introduction

This section describes the procedure to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.0.1 for existing Communication Manager on S8300B or S8300C Server.

In this upgrade procedure, replace the S8300B or S8300C Server by an S8300D server running System Platform and the embedded survivable remote template.

The embedded survivable remote template supports the utility services.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

Perform the following upgrade tasks for all servers on releases of Communication Manager earlier than 5.2.1.

1. Upgrade the S8300 server to Communication Manager Release 4.0.5 or Release 5.2.1.

   For servers that you can upgrade directly to Release 4.0.5 or Release 5.2.1, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

   S8300A servers require special procedures to upgrade.
2. Install a preupgrade patch to Release 4.0.5 or Release 5.2.1 in preparation for the upgrade to Release 6.0.1.
3. Perform the upgrade to Release 6.0.1 as described in this section.

Preupgrade tasks on S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.

      The configuration screen appears in your application window.

   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**
   - **Phone Message File**

     If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.
8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Checking the availability of the FTP, SFTP, or SCP server

Prerequisites

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP (for release 1.x, 2.0 or 2.0.1, the system supports only FTP) server over the customer LAN. You require a current version of the system data to restore the system configuration after you complete the upgrade.

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging in from a laptop directly connected to the services port, perform one of the following:
    - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
    - If you are using Telnet, enter `telnet 192.11.13.6 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

     Note:
     For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
   - If Communication Manager Messaging is enabled:
     1. Select **Specify Data Sets**.
     2. Select the following check boxes:
        - **Avaya Call Processing (ACP) Translations**
        - **Server and System Files**
        - **Security Files**
        - **Communication Manager Messaging (CMM)**

          Select **Translations, Names, and Messages**.
     3. In the **Download size** field, enter the size of the backup `.tar` file.

        There could be more than one `.tar` file if the backup size is large.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:

- **User Name**
- **Password**
- **Host Name**. Enter the host IP address.
- **Directory**

  When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.

5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     1. Select the **Update ID** and click **Unpack**.
     2. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     1. Select the **Update ID** and click **Activate**.
     2. The system displays the status as the update progresses. The system automatically reboots, if required.
     3. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**

- **Host Name**
- **Directory**

  The backup location must be a server on the customer LAN.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   Caution:

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the devices from the server

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the server

Prerequisites

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.
- Connect the USB CD/DVD drive.
- Insert the System Platform media.

⚠ **Caution:**

Ensure that you wear a properly grounded ESD wrist strap when handling the server. Place all components on a grounded, static-free surface when working on them.

1. Loosen the two thumb screws on the faceplate of the server.
2. When removing the server, remove the LED panel (above slot V1) (G700 only) or the space bar (G250, G350 and G450) with the server.
    - For G700, disengage the LED panel and the server, and remove them together from the branch gateway.
    - For G250, G350 or G450, remove the space bar and the server.
    - For G430, remove the server from the branch gateway.
3. Perform one of the following:
    - For G700, partially reinsert the LED panel (above slot V1) and the new S8300D server (slot V1). Leave them extended from the branch gateway by about 1 inch (2.5 cm).

      Do not seat these circuit packs now.

- For G250, G350, G430 and G450, partially reinsert the new S8300D Server (slot V1). Leave the server extended from the branch gateway by about 1 inch (2.5 cm). Do not seat this circuit pack now.

4. With the S8300D in slot V1 still extended, by about 1 inch (2.5 cm), connect the USB CD/DVD drive to any one of the USB ports.
5. When you are ready to start installing System Platform, seat the S8300D Server (for G700, also seat the LED panel) into the branch gateway by gently pressing it until the faceplate is aligned with the face of the branch gateway.
   a. Insert the System Platform media into the USB CD/DVD drive within by about 30 seconds of seating the S8300D Server.
   b. If the media is not present in the CD/DVD drive or if the USB CD/DVD drive is not connected to the server at the time of boot, you must repeat the Step 5.

      Alternatively, reboot the server by powering up and powering down the branch gateway.

      When the server starts to boot, it looks for the software on the DVD/CD-ROM. The Alarm LED of the S8300 Server is steady as it is starting. The Alarm LED starts flashing when the S8300 Server is ready to load software.
6. Secure the faceplate of the S8300D server with the thumb screws. Tighten the thumb screws with a screw driver. For G250, G350, and G450, secure the space bar above slot V1
7. Reconnect the laptop to the services port of the new S8300D server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

Note:

If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

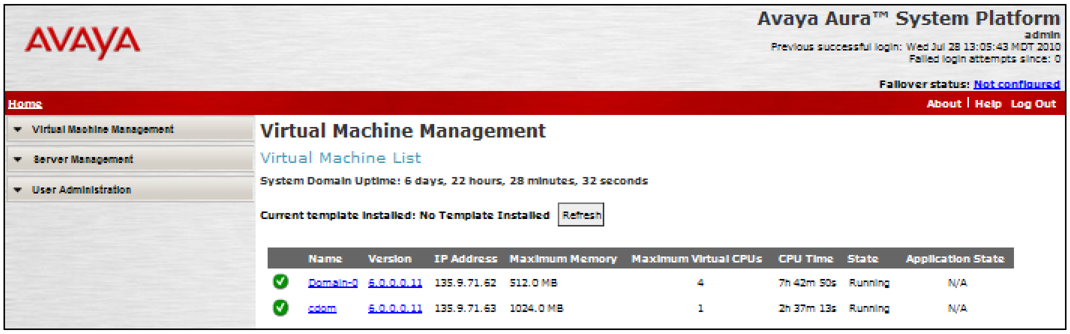
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed [Refresh]

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   ✱ **Note:**

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   ✱ **Note:**

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Configuring the alarming information

Prerequisites

Log on to System Management Interface.

Configure the information provided in the worksheet available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Configure the following alarm information:
    - **Alarms** > **SNMP Agents**
    - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

    For more information, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431).

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

    The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Submitting the scheduled backups

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. On the Schedule Backup Web page, select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:

- **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8400 Server configured as survivable remote processor, formerly Local Survivable Processor (LSP) running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.0.1 on S8300D Server.

In this procedure:

- You discard:
    - All circuit packs
    - The G600, G650 Media Gateway or the CMC cabinet
- You install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

The upgrade procedure involves:

- Creating a data set to use if you have to back out of the upgrade.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

You require a new license for Communication Manager Release 6.0.1.

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.0.1. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D Server.

Preupgrade tasks on the S8400 Server

Connecting to the server

Prerequisites

A CAT5 cross-over cable to connect your services laptop to the server.

1. Plug one end of the CAT5 cross-over cable into the services access port on the server faceplate.
2. Plug the other end of the cross-over cable into the services laptop.
3. Start a SAT session.
4. Log in as `craft`.

Accessing System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

You back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

If Communication Manager Messaging is enabled on your system, back up the messaging data.

Backing up the files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
   - **Avaya Call Processing (ACP) Translations**
   - **Server and System Files**
   - **Security Files**
   - **Communication Manager Messaging (CMM)**

     Select **Translations, Names, and Messages**.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Prerequisites

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

⚠ **Electrostatic alert:**

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.

11. Connect a laptop to the services port of the S8300 Server using a crossover cable.
12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

   c. In the command line, type **`service_port_access enable`** and press **Enter**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

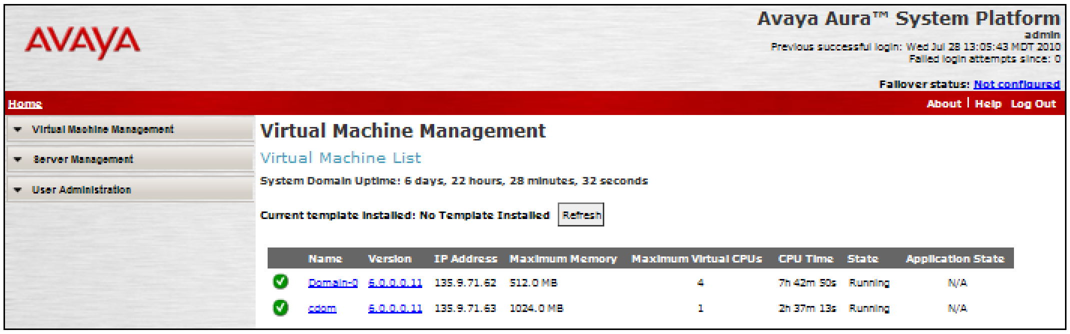
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**

- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:

     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

Prerequisites

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Enter `add media-gateway <number>`, where <*number*> is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:

   - Enter `show system`.
   - Note the serial number of the branch gateway.

     The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.
4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   Note:

   The subnet mask for the branch gateway must be the same as that of the S8300D Server.
5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.
6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.

5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

  Note:

  Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Completion tasks on the S8400 Server

Shutting down the server

1. Push and hold the **Shutdown** button on the faceplate of the server for more than 2 seconds.

   The **OK to Remove LED** in green flashes to indicate that shutdown is in progress.
2. When the green **OK to Remove LED** is steady, unlatch the circuit pack, slide it out of its slot.
3. Leave the compact flash card with translations in the slot.
4. Leave cable adapter of the server attached at the rear of the carrier and its cable connections in place during the entire replacement procedure.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Turning off the power to the port network

1. From the bash prompt on the services laptop, enter `shutdown system` and press `Enter`.

   This shuts down the server gracefully.
2. Wait until the **Shutdown Complete** LED on the lower portion of the faceplate of the server is solid green.
3. Turn off the power to the media gateway for safety purpose.

⚠ **Danger:**

The latch on the power supply acts as the DC power switch and removes only DC power from the backplane. To remove the AC power from the media gateway, pull the AC power cord from the back of the media gateway.

4. Unplug the power cord for safety purpose.

Upgrading S8500 Server to the S8300D Server

Introduction

This section describes the procedure to upgrade the existing S8500 Server configured as survivable remote processor, formerly Local Survivable Processor (LSP) running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.0.1 on S8300D Server.

In this procedure:

- You discard:
  - All port networks (CMCs, SCCs, MCCs or IP600)
  - All circuit packs and any gateways above 50
  - The S8500 Server and the G650 Media Gateway
- You install a G430 or G450 Branch Gateway with an S8300D Server running System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

The embedded survivable remote template supports Utility Services.

The upgrade procedure involves:

- Creating a data set to use if you have to back out of the upgrade.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers. You do not require to restore the translations manually.

You require a new license for Communication Manager Release 6.0.1.

You can upgrade Communication Manager running releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first, before you upgrade to Release 6.0.1. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on S8300D Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the following required hardware: • S8300D Server • G430 or G450 Branch Gateway • Media modules	
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.
	One of the following as appropriate: • *Installing and updating the Avaya G450 Media Gateway* (03-602054) • *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053) • *Installing and updating the Avaya G430 Media Gateway* (03-603233) • *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)	Provides instructions for installing and configuring the G450 or G430 Branch Gateway and installing the S8300D Server.

Preupgrade tasks on the S8500 Server

Upgrading branch gateways and survivable servers

If newer firmware exists for a configuration using H.248 branch gateways and media modules, you must upgrade the firmware on the branch gateways.

If the server being upgraded is the main server for a system that includes survivable servers, upgrade the survivable servers first.

Upgrade the branch gateways and survivable servers to the latest version in the following sequence:

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on survivable remote server (formerly local survivable processors)
4. Communication Manager on survivable core server (formerly enterprise survivable servers)
5. Communication Manager on a main server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

      If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
    - LAN access by host name

      If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
    - Portable computer access by IP address

      If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

     Note:

     For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:

     - **Avaya Call Processing (ACP) Translations**

- **Server and System Files**
- **Security Files**

- If Communication Manager Messaging is enabled:

  i. Select **Specify Data Sets**.

  ii. Select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
  - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.

  iii. In the **Download size** field, enter the size of the backup `.tar` file.

  There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Prerequisites

Install G450 or G430 Branch Gateway. For information to install the branch gateway, see one of the following documents:

- *Installing and updating the Avaya G450 Media Gateway* (03-602054) and *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Installing and updating the Avaya G430 Media Gateway* (03-603233) and *Quick Start for Hardware Installation: Avaya G430 Media Gateway* (03-603236)

Electrostatic alert:

ESD can damage electronic circuits. Do not touch the server unless you wear a grounding wrist strap or other static-dissipating device. Place all components on a grounded, static-free surface when working on them.

1. Connect the DVD/CD-ROM drive using the USB cable to one of the USB ports on the faceplate of the S8300D Server.
2. Insert the System Platform media into the external USB CD/DVD drive.
3. Remove the blank plate from slot V1.
4. Position the S8300 Server before the V1 bay opening and engage both sides of the server in the interior guides of the gateway.
5. Slide the S8300 Server slowly into the chassis.

   Maintain an even pressure to ensure that the server does not become twisted or disengaged from the guides
6. Apply firm pressure to engage the connectors.
7. Tighten the spring-loaded captive screws on the front of the S8300 Server to lock the server into the chassis.
8. Insert each module needed for your configuration in a slot appropriate for that module.

   Note:

   Media modules are restricted to certain slots.
9. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

10. Turn on the branch gateway.

    The PWR LED on the front panel lights, indicating the operational status of the power supply unit. When the LED turns green, it indicates that the power is applied to the unit.

11. Connect a laptop to the services port of the S8300 Server using a crossover cable.

12. Connect the laptop to the services port of the S8300D Server.

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:

    a. Start an SSH session.

    b. Log in to System Domain (Domain-0) as admin.

   c. In the command line, type **`service_port_access enable`** and press **Enter**.

2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

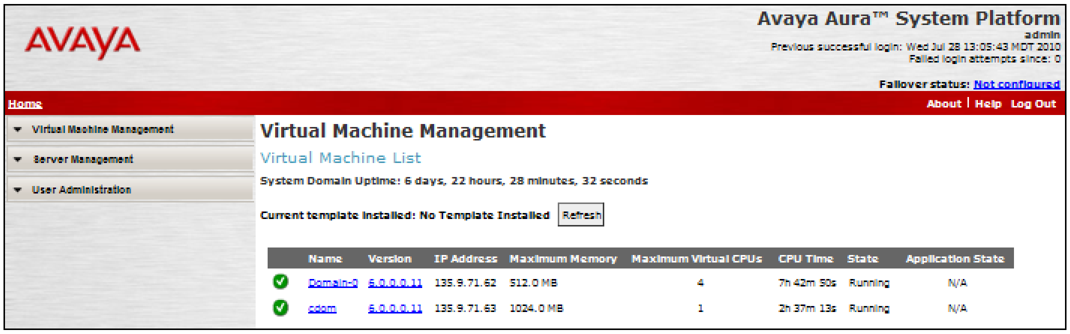
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**

- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Configuring a branch gateway

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Connect the laptop computer to the services port of the branch gateway using an Ethernet cable.
2. At the command prompt, enter the user ID and the password.
3. Enter `y` to configure basic gateway connectivity.
4. Configure the following parameters:
   - VLAN number
   - IP address and subnet mask for the primary management interface

     Note:
     The subnet mask for the branch gateway must be the same as the subnet mask for the S8300D Server.
   - IP address for the default gateway (router)
   - Up to four IP addresses to specify the Media Gateway Controllers
   - Hostname for the branch gateway

   The system displays the settings you configured and prompts you to confirm the settings. After you confirm the settings, the system saves them and the branch gateway reboots.
5. Perform the following tasks to register the branch gateway with Communication Manager:
   a. Enter `add mgc list` *`IP of CM procr / clan`*.
   b. Enter `copy running-config startup-config`.
   c. Enter `reset`.

Adding a branch gateway in Communication Manager

Prerequisites

- Register the branch gateway with Communication Manager.
- Start a SAT session.

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Enter `add media-gateway <number>`, where <*number*> is the gateway number between 1 to 50.
2. In the **Name** field, enter the hostname assigned to the branch gateway.
3. In the **Serial No** field, enter the serial number of the branch gateway.

   To obtain the serial number of the branch gateway, on the command prompt of the gateway:

   - Enter `show system`.
   - Note the serial number of the branch gateway.

     The serial number is case-sensitive, and if entered incorrectly, the system prevents the S8300D Server from communicating with the branch gateway.
4. Save the changes.

   If properly administered, the branch gateway registers with the main server within 1–2 minutes. The system populates the values in the **IP Address**, **MAC Address**, and the **Module Type** fields after the branch gateway registers with the server.

   > **Note:**
   >
   > The subnet mask for the branch gateway must be the same as that of the S8300D Server.
5. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the branch gateway number.

   The system lists the media modules installed in the media next to their slot numbers. Verify that the gateway is successfully added.
6. Enter `list media-gateway` and verify that **Reg?** field is set to `y`.

   The `y` in the **Reg?** field signifies that the branch gateway is registered. The system does not register the gateway:

   - If the serial number administered in the **Serial No** field on the **`change media-gateway`** screen is incorrect
   - If the IP connection between the branch gateway and the S8300D Server is not established
   - If the branch gateway is not registered with Communication Manager

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.

5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   ❗ **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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.

- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

  Note:
  Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Removing the G650 Media Gateway and the circuit packs

Discard any hardware you replaced during the upgrade.

1. Remove the G650 Media Gateway from the rack.
2. Discard all the circuit packs you removed from the gateway or the port network.

Registering the system

Use the standard procedure to register the system.

Completion tasks on S8500 Server

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting from the server

Unplug the laptop from the services port.

Removing the server from the rack

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

   For more information, see *Quick Start for Hardware Installation: Avaya S8500 Server*.

Upgrading the S8300D server to S8300D server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 to Release 6.0.1 on an S8300D server.

In this procedure, you upgrade the existing S8300D to run System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

The embedded survivable remote template supports the utility services.

Communication Manager does not support upgrading SIP Enablement Services (SES) to Release 6.0.1.

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 5.2.1.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.0.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration. You require a new license file for Communication Manager Release 6.0.1.

For S8300D servers on releases of Communication Manager earlier than 5.2.1, upgrade to Release 5.2.1 first before you upgrade them to Release 6.0.1. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Onsite preparation

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
   a. Right-click and select **Paste**.

      The configuration screen appears in your application window.
   b. Click **File** and select **Save As**.
   c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
   d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
   - **Server Role**
   - **Set Identities**
   - **Configure Interfaces**
   - **Set DNS/DHCP**
   - **Set Static Routes**
   - **Configure Time Server**
   - **Server Access**
   - **Server Date/Time**

- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.
2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.
   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging in from a laptop directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.

   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

Prerequisites

Log on to System Management Interface.

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, perform one of the following:
   - If Communication Manager Messaging is not enabled:

     Select **Full Backup**.

     The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging.

> **Note:**
>
> For Communication Manager Release 1.x, 2.0 or 2.0.1, because **Full Backup** option is not available, select the following check boxes:
>
> - **Avaya Call Processing (ACP) Translations**
> - **Server and System Files**
> - **Security Files**

- If Communication Manager Messaging is enabled:

  i. Select **Specify Data Sets**.

  ii. Select the following check boxes:

  - **Avaya Call Processing (ACP) Translations**
  - **Server and System Files**
  - **Security Files**
  - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.

  iii. In the **Download size** field, enter the size of the backup `.tar` file.

  There could be more than one `.tar` file if the backup size is large.

3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**. Enter the host IP address.
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the `/var/home/ftp/pub` location. You must move the file to the services laptop before you proceed with the upgrade.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

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

   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.

    ii. Wait until the system displays the message, `... unpacked successfully`.

  - If the status of the update file you want to activate is unpacked:

    i. Select the **Update ID** and click **Activate**.

    ii. The system displays the status as the update progresses. The system automatically reboots, if required.

    iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
3. Click **Submit**.

    The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**
    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Verify if the **Restart server after shutdown** check box is selected.

Disconnecting the devices from server

Disconnect the USB CD/DVD reader from the server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license

  Note:

  If you are upgrading a survivable remote server, do not install the Communication Manager license file.

- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

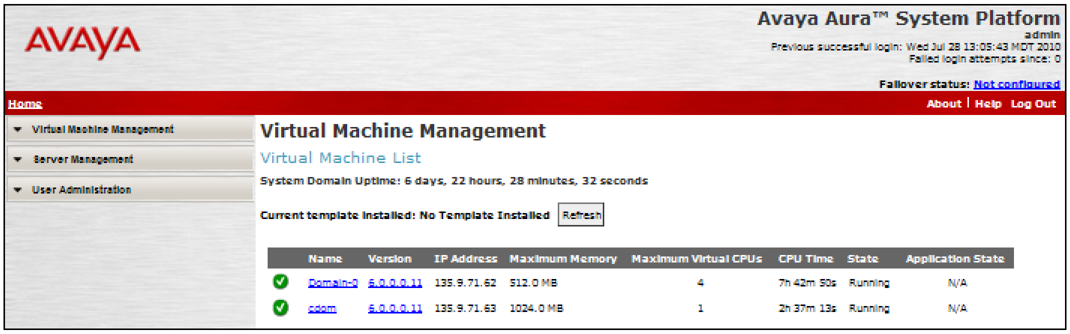
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed Refresh

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Configuring the alarming information

Prerequisites

Log on to System Management Interface.

Configure the information provided in the worksheet available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter `almsnmpconf` to enter any data that you recorded earlier.

   For more information, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers* (03-300431).

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.

4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.
   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Submitting the scheduled backups

1. On the System Management Interface, under **Data Backup/Restore**, click **Schedule Backup**.
2. On the Schedule Backup Web page, select the scheduled backup and click **Change**.
3. On the Change Current Schedule page, click **Change Schedule**.
4. Repeat steps 2 and 3 for all the scheduled backups.

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:

- **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

  Note:

  Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Chapter 8: Converting to port network

Upgrading DEFINITY Server CSI in CMC to the S8800 Server

Introduction

This section describes the procedure to upgrade the existing DEFINITY Server CSI in a CMC to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.0.1. You reuse the cabinet in the new system.

In this procedure, you replace the DEFINITY Server CSI with S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex main/survivable core template (CM_Simplex).

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.0.1.

- Administering IPSIs on Communication Manager Release 6.0.1.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1. This upgrade affects service because you turn off the cabinets to replace the processor and tone-clock circuit packs. The system drops all calls, the service returns when the server takes control of the IPSIs.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.	STS updates the translations to the latest version. This process can take two weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For information on where and how to send the translations and forms to be used, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following servers, as appropriate: - S8800 Server - Dell™ PowerEdge™ R610 Server - HP ProLiant DL360 G7 Server • Circuit packs: - TN2312BP IPSI	

✔	Task	Description
	- TN2602AP or TN2302AP Media Processor - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site available at http://avaya.com/support.
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.

- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. The changing or upgrading the hardware includes:

- Adding new TN2312BP IPSI, TN799D C-LAN, and TN2302 or TN2602 Media Processor circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Replacement of circuit packs

The TN2312BP IPSI circuit pack in the PN replaces the existing circuit packs and terminates control communication with the server. CAT5 Ethernet cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit pack, program static IP addresses into the IPSI.

You can complete this task at any time before the cutover. IPSI circuit pack is hot swappable, and you replace the circuit pack in the existing DEFINITY system without the need to turn off the power.

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSI is working in the existing system.
- Test the connectivity between the server and the IPSI.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Prerequisites

Cross-over cable.

1. Connect your Services laptop directly to the processor to access the cabinet.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).
- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
    a. Start an SSH session.
    b. Log in to System Domain (Domain-0) as admin.
    c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

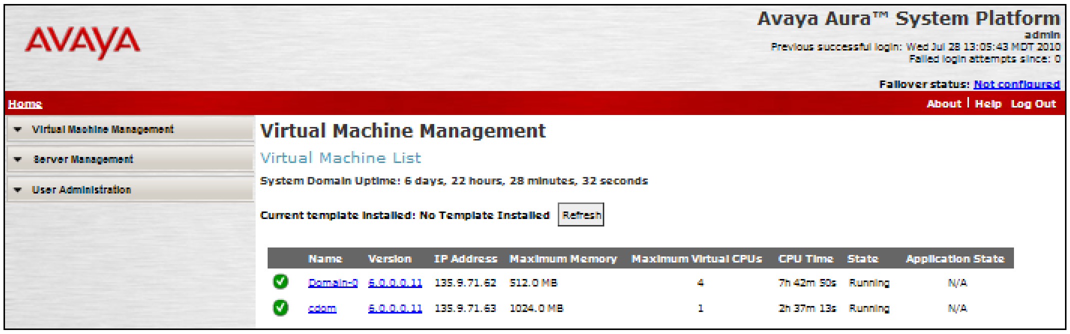
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the translations

Prerequisites

Log in to System Management Interface.

Use this procedure to restore translations only on the main server. When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

1. Under **Administration**, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**

- If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
- If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.

- Click **Local Directory** and provide the path to the backup file on your local directory.

Important:
If the server is not connected to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   Important:
   Do not restore a file with a name that starts with a "os_" or "full_". Restore only the files with the extension `.xln`.

6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the Restore status.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
   a. Select **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.

The system displays the Messaging Administration screen.

3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.
   You can select four files at a time from the language CD that you want to copy to the server.

6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   1. In the **Name** field, enter `tmp`.
   2. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   1. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   2. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   1. In the **Name** field, enter `msgserver`.
   2. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   1. In the **Far-end Node Name** field, enter `msgserver`.
   2. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

   For more information, see About subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.

4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.
6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.

   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.

   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.
9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
   - TN2312BP IPSI
   - TN799DP Control-LAN (C-LAN)
   - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you might also need to adjust the administration of the network regions. Your planning documents might provide information about changes to network regions. For more information on how to administer network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit packs

Prerequisites

Start a SAT session.

Complete Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6
     - DiffServ: 46
3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

   Important:

   Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.

3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
    a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
    b. Complete each field with the information for this circuit pack.

    If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
    a. Enter `add data-module next`.
    b. In the **Type** field, enter `ethernet`.
    c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

    The default is **none**.

Disconnecting from the server

Unplug the laptop from the services port.

Postupgrade tasks on S8800 Server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.

3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:
     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

Note:

Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading DEFINITY ONE/S8100 in CMC to the S8800 Server

Introduction

This section describes the procedure to upgrade the existing S8100 Server in a CMC to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.0.1. You reuse the cabinet in the new system.

In this procedure, you replace:

- The TN2314 or TN795 circuit pack with a TN2312BP IPSI circuit pack
- The S8100 Server with an S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex main/survivable core template (CM_Simplex)

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.0.1.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1. This upgrade affects service because you turn off the cabinets to replace the processor circuit pack. The system drops all calls, the service returns when the new server takes control of the IPSIs.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.	STS updates the translations to the latest version. This process can take two weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For information on where and how to send the translations and forms to be used, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following servers, as appropriate: - S8800 Server - Dell™ PowerEdge™ R610 Server - HP ProLiant DL360 G7 Server • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site available at http://avaya.com/support.
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. The changing or upgrading the hardware includes:

- Adding new TN2312BP IPSI, TN799D C-LAN, and TN2302 or TN2602 Media Processor circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Replacement of circuit packs

The TN2312BP IPSI circuit pack in the PN replaces the existing circuit packs and terminates control communication with the server. CAT5 Ethernet cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit pack, program static IP addresses into the IPSI.

You can complete this task at any time before the cutover. IPSI circuit pack is hot swappable, and you replace the circuit pack in the existing DEFINITY system without the need to turn off the power.

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSI is working in the existing system.
- Test the connectivity between the server and the IPSI.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Prerequisites

A cross-over cable to connect your services laptop directly to the processor.

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list trunk-group`.

This command displays every trunk group administered on the system.

3. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Recording IP settings

Prerequisites

Start a Telnet session to access the processor circuit pack that is connected to the service laptop.

You must view and record the IP settings assigned to the processor that you must configure on the new server. For this, use the worksheet provided in Appendix A.

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log on as `craft` or `dadmin`.
4. Enter `setip`. The system displays the list of IP settings.
    - cust: IPaddress, subnet mask, gateway
    - dns: server name, domain name, 2 DNS server IP addresses
    - wins: two WINS server IP addresses
    - ras: one remote access server IP address
5. Record this information exactly as displayed.

    Important:

    Include any periods, commas, or other punctuation marks. Record this information in lowercase or uppercase as the information appears.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).

- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.

4. Click **Continue**.

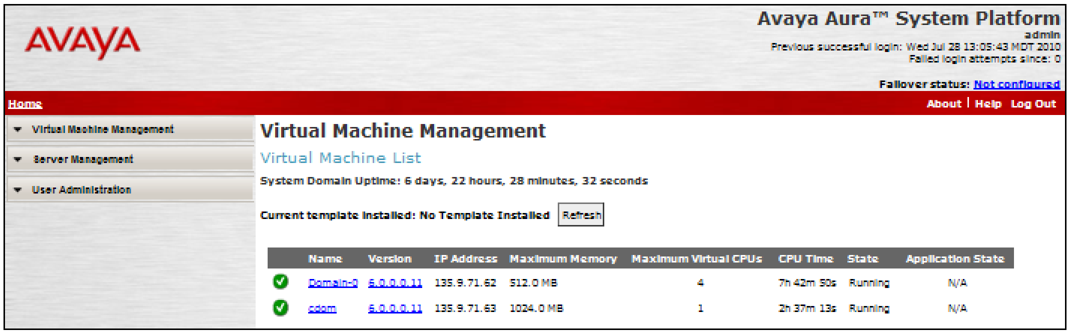
5. Enter a valid password.

6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:

- LAN access by IP address

  If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.

- LAN access by host name

  If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I’m using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the translations

Prerequisites

Log in to System Management Interface.

Use this procedure to restore translations only on the main server. When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

1. Under **Administration**, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**

  - If you selected FTP or SFTP in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
  - If you selected SCP in the **Method** field, enter the full path of the file in the **File Path** field.
- Click **Local Directory** and provide the path to the backup file on your local directory.

> **Important:**
> If the server is not connected to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

> **Important:**
> Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.

6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the Restore status.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.

The Messaging Software page displays `Internal messaging is disabled`.

b. Click **Enable**.

The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
    - File(s) to download from the machine I'm using to connect to the server.
    - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the RFU.
    - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.

The system displays the Messaging Administration screen.

3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:
   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.
   You can select four files at a time from the language CD that you want to copy to the server.

6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
    a. In the **Name** field, enter `tmp`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
    This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
    a. Record the value of the **Far-end Node Name** field.
    You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
    b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
    a. In the **Name** field, enter `msgserver`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
    a. In the **Far-end Node Name** field, enter `msgserver`.
    b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.
    Remove the entries from the **Name** and **IP Address** fields and submit the form.
    This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

   For more information, see About subnet address.

3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the cabinet

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.
6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

d. Enter `reset` and press `Enter`.

   Add or copy the login portion before you add the control gateway.

9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Turning off the power to the control cabinet

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

   The green light indicates that the cabinet is shut down.

   Important:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.

2. Remove the power cord from the back of the cabinet.
   The cabinet turns off.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
    - TN2312BP IPSI
    - TN799DP Control-LAN (C-LAN)
    - TN2302AP or TN2602AP IP Media Processor

    If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Prerequisites

Start a SAT session.

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:

- 802.1p: 6
- DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:

Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

The default is **none**.

Postupgrade tasks on S8800 Server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:

- *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
- *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

Important:

The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

Note:

Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading Avaya IP600/S8100 Server in G600 to the S8800 Server

Introduction

This section describes the procedure to upgrade the existing S8100 Server in G600 Media Gateway to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.0.1. You reuse the cabinet in the new system.

In this procedure, you replace:

- The TN2314 or TN795 circuit pack with a TN2312BP IPSI circuit pack
- The S8100 Server with an S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex main/survivable core template (CM_Simplex)

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Saving and freezing translations.
- Sending the translations to the STS team few weeks before the upgrade and obtaining the updated translations from STS.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.0.1.
- Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1.

This upgrade affects service. When you turn off the PPN stack to replace the cabinet as part of the upgrade process, the system drops all calls. Service returns when the new server takes control of the IPSIs. Before you turn off the cabinets, perform the following administration tasks.

Prerequisites

Preupgrade checklist

Before you start the upgrade, perform the following tasks:

✔	Task	Description
	Send the translations to the STS team few weeks before the upgrade and obtain the updated translations from STS.	STS updates the translations to the latest version. This process can take two weeks. STS returns the translation reports and translation files to the project manager by e-mail who sends them to the technical support representative. For information on where and how to send the translations and forms to be used, contact the STS scheduling desk at 720-444-9418.
	Verify that you have the required software: • System Platform • Communication Manager	
	Obtain the required hardware: • One of the following servers, as appropriate: - S8800 Server - Dell™ PowerEdge™ R610 Server - HP ProLiant DL360 G7 Server • Circuit packs: - TN2312BP IPSI - TN2602AP or TN2302AP Media Processor - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from

✔	Task	Description
		the Avaya Support Web site available at http://avaya.com/support.
	Ensure that you have the required customer-provided network information.	

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.
	Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	Provides instructions for administering network regions.

Preupgrade tasks

Preupgrade setup

You must complete the following tasks onsite about two weeks before you start the actual upgrade. If you do not complete these tasks, do not continue with the upgrade.

- Freeze the translations.
- Send the translations to the STS team. STS updates the translations to the latest version and sends the translation reports and translation files.
- Obtain the updated translations from STS by e-mail.
- Save the translations so you can access the file from the new system, for example, on you computer.

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. The changing or upgrading the hardware includes:

- Adding new TN2312BP IPSI, TN799D C-LAN, and TN2302 or TN2602 Media Processor circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Saving translations

Prerequisites

Start a SAT session.

Avaya recommends that you perform this procedure for safeguarding the system, in case you need to bring the system to its current configuration.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Replacement of circuit packs

The TN2312BP IPSI circuit pack in the PN replaces the existing circuit packs and terminates control communication with the server. CAT5 Ethernet cables provide connectivity that is unavailable by the backplane of older carriers. After you install the IPSI circuit pack, program static IP addresses into the IPSI.

You can complete this task at any time before the cutover. IPSI circuit pack is hot swappable, and you replace the circuit pack in the existing DEFINITY system without the need to turn off the power.

- Connect the IPSIs by CAT5 cable to the server complex to customer network.

  You can perform this while the IPSI is working in the existing system.
- Test the connectivity between the server and the IPSI.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Preupgrade administration

Connecting to the processor

Prerequisites

A cross-over cable to connect your services laptop directly to the processor.

1. Perform one of the following tasks to connect the services laptop to the processor:
   - If the processor circuit pack is a TN795, insert the NIC card into the slot on the faceplate.
   - If the processor circuit pack is a TN2314, plug the RJ45 connector into the RJ45 jack on the faceplate.
2. Start a SAT session.
3. Log in as `craft`.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
3. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Recording IP settings

Prerequisites

Start a Telnet session to access the processor circuit pack that is connected to the service laptop.

You must view and record the IP settings assigned to the processor that you must configure on the new server. For this, use the worksheet provided in Appendix A.

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log on as `craft` or `dadmin`.
4. Enter `setip`. The system displays the list of IP settings.
   - cust: IPaddress, subnet mask, gateway
   - dns: server name, domain name, 2 DNS server IP addresses
   - wins: two WINS server IP addresses
   - ras: one remote access server IP address
5. Record this information exactly as displayed.

   Important:

   Include any periods, commas, or other punctuation marks. Record this information in lowercase or uppercase as the information appears.

Upgrade tasks

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).

- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura ™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:
You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

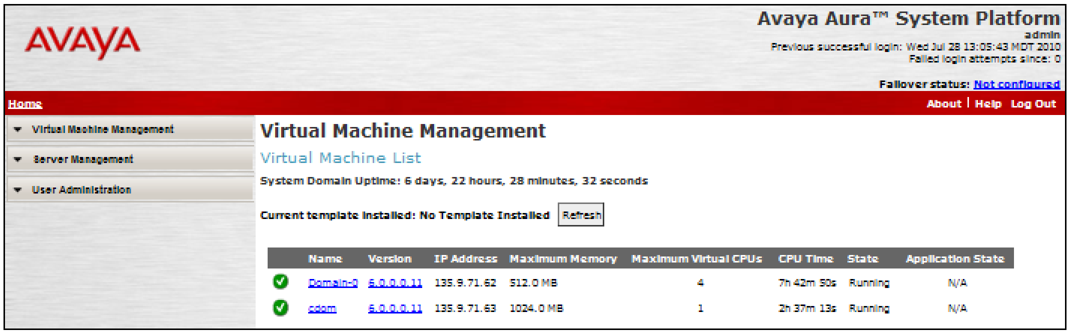
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.


AVAYA
Avaya Aura™ System Platform
admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:
   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two

ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the translations

Prerequisites

Log in to System Management Interface.

Use this procedure to restore translations only on the main server. When the survivable core server or survivable remote server registers with the main server, the main server sends a copy of the translations to the survivable servers.

1. Under **Administration**, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

   ❗ **Important:**

   If the server is not connected to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the file to restore, for example, `*_cmserver1_*.xln`.

   ❗ **Important:**

   Do not restore a file with a name that starts with a “os_” or “full_”. Restore only the files with the extension `.xln`.
6. Select both the options of **Force**.
7. Click **Restore**.
8. Click **Restore History** and select the file that you want to restore.
9. Click **Status** to view the Restore status.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    1. Select **Miscellaneous** > **Messaging Software**.

       The Messaging Software page displays `Internal messaging is disabled`.
    2. Click **Enable**.

       The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
    - File(s) to download from the machine I’m using to connect to the server.
    - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the RFU.

- Enter the URL to download the RFU and enter the host name and domain name of the proxy server.

5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form. This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.

6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

   For more information, see About subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the G600 gateway

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.

6. Close the IPSI session and log in to the IPSI:
    a. Enter `exit`.

       The system saves the changes and ends the IPSI session.
    b. Enter `192.11.13.6` and log in to the IPSI.
    c. Enter `show control interface`.

       The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
    d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
    a. Enter `exit`.

       The system saves the changes and ends the IPSI session.
    b. Enter `192.11.13.6` and log in to the IPSI.
    c. Enter `show control interface`.

       The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
    d. Enter `reset` and press `Enter`.

       Add or copy the login portion before you add the control gateway.
9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Turning off the power to the control cabinet

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

   The green light indicates that the cabinet is shut down.

   Important:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.

2. Remove the power cord from the back of the cabinet.
   The cabinet turns off.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Replacing I/O cables

Prerequisites

Turn off power to the carrier or the media gateway.

⚠ **Caution:**

Failure to turn off the power can result in electric shock.

On older G600 cabinets you must replace the existing I/O cables (WP-90753, LI), which connect the backplane to the rear connector panel, with twisted pair I/O cables. The existing I/O cables have straight wires. They may be white with two red wires, or multicolored wires. If the cables have multicolored, tightly twisted wires do not replace them.

⚠ **Electrostatic alert:**

When you add or replace any hardware and associated cables and adapters, wear a grounded wrist strap to ground yourself against electrostatic discharge (ESD). Failure to follow ESD procedures can result in system damage or service disruption.

1. For the G600 Media Gateway, remove the fan assembly to access the cables.
   a. Loosen the thumb screws on the fan assembly and pull it out.
   b. Leave the fan assembly off until all the wires are installed.
2. Note the orientation of the existing I/O cables.

   The existing I/O cables may be white and red or multicolored. They are not twisted.
3. Remove the nontwisted pair of existing I/O cables from the backplane and the connector panel slots.
4. Install the 10 tight-twisted pair I/O cables onto the backplane.

   Observe the white outline printed on the backplane for the location of each connector.
5. When you view from the side with twin connectors (that is, while plugging them into the backplane) and with the connectors oriented properly for plug-in, they should look like

   The connector panel contains some pin locations that have no wires in them. Top of the connector panel contains an orange-black pair on the right and a violet-brown pair on the left. The 50-position metal shell D connectors should be installed into the connector panel with the longer side of the D (pins 1–25) toward the right when viewed from the rear of the media gateway.
6. For the G600 Media Gateway, perform one of the following:
   - If you do not have to install any other gateway, replace the fan unit .

- If you have to add more gateways to the rack, leave the fan units off until all of the TDM cables are installed.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
    - TN2312BP IPSI
    - TN799DP Control-LAN (C-LAN)
    - TN2302AP or TN2602AP IP Media Processor

   If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack` *`n`*, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface` *`PNnumber`*, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.

3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Prerequisites

Start a SAT session.

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:
    - 802.1p: 6
    - DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
    - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
    - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
        - **802.1p (vlan priority)**: `6`
        - **DiffServ**: `46`

- **Auto** (port negotiation): `y` for the following default values:
  - `Full duplex`
  - `100mbps` speed
- **Auto** (port negotiation): `n` to modify as per the network configuration.
  - **Duplex full**
  - **Speed 100**

3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

   Important:

   Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.

6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.

7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.

3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.

5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.

c. Complete the remaining fields on the window.

6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Postupgrade tasks on S8800 Server

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.
2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.
3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.
4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.
5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Prerequisites

Log on to System Management Interface.

1. Under **Alarms**, click **Current Alarms**.
2. Under **Server Alarms**, select the alarms to be cleared.
3. Click **Clear**.
4. Use a SAT session to resolve new alarms after the server upgrade. For more information, see:
   - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers, 03-300431*
   - *Avaya Aura™ Communication Manager Server Alarms, 03-602798.*

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:

- **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
- **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
- **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.

6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Disconnecting from the server

Unplug the laptop from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading S8300 Server to the S8800 Server

Introduction

This section describes the procedure to upgrade the embedded S8300 Server in G430 or G450 Branch Gateway to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server.

In this upgrade scenario:

- You discard the embedded S8300 Server and the H.248 Branch Gateway.
- You install a G650 Media Gateway and move the supported circuit packs to the media gateway that becomes a port network on the new system running Communication Manager Release 6.0.1.
- You install the standalone S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex main/survivable core template (CM_Simplex).

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.
- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Restoring the data set on Communication Manager Release 6.0.1.
- Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Installing G650 Media Gateway.

- Adding circuit packs to the media gateway.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1.

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.0.1. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on the S8800 Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the Communication Manager template (as appropriate)	
	Obtain the required hardware: • One of the following servers, as appropriate: - S8800 Server - Dell™ PowerEdge™ R610 Server	

✔	Task	Description
	- HP ProLiant DL360 G7 Server • Circuit packs: - TN2312BP IPSI - TN799DP C-LAN	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Preupgrade tasks on the S8300 Server

Accessing the System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. Depending on the server configuration, choose one of the following:
    - LAN access by IP address

      If you are logging on to the corporate local area network, enter the unique IP address of Communication Manager in standard dotted-decimal notation.
    - LAN access by host name

If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

- Portable computer access by IP address

  If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying the current software release

1. Under **Server**, click **Software Version**.

   The system displays the Software Version page.

2. Verify that the **CM Reports as:** field displays one of the following:
   - `R014x.00.5.742.0` for Communication Manager Release 4.0.5

     This means that Communication Manager Release 4.0.5 is running on the server.

   - `R015x.02.1.016.4` for Communication Manager Release 5.2.1

     This means that Communication Manager Release 5.2.1 is running on the server.

Copying configuration information

You need to record the configuration information found on System Management Interface and use it to configure Communication Manager after the upgrade. You cannot complete the server upgrade without the configuration information. You can manually copy the information on each screen to a worksheet, copy and save each screen to your computer, or print each screen.

Viewing and copying the configuration screens

Prerequisites

- Create a new folder on your computer to store the configuration files. Storing the files in a new folder makes them easier to find.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

The system backs up most of the server data and restores it after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix of this book.

1. Under **Installation**, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard screen.
3. Select **Configure all services using the wizard** and click **Continue**.
4. Press `Alt` +`PrintScrn` on your keyboard.
5. Start the application (Microsoft Word, Wordpad, or Microsoft Paint), on which you want to copy the configuration and perform the following:
    a. Right-click and select **Paste**.
    The configuration screen appears in your application window.
    b. Click **File** and select **Save As**.
    c. Select the folder that you created. In the **File Name** field, change the name of the file to match the configuration screen that you copied.
    d. Click **Save**.
6. Click **Administration** > **Server (Maintenance)**.
7. Print or copy the information from the following screens:
    - **Server Role**

- **Set Identities**
- **Configure Interfaces**
- **Set DNS/DHCP**
- **Set Static Routes**
- **Configure Time Server**
- **Server Access**
- **Server Date/Time**
- **Phone Message File**

  If the system displays any unicode message files installed on the system, you need to reinstall these files after the upgrade.

8. After you copy or print the Configure Server screens, click **Cancel**. *Do not* click **Submit**.
9. On the command line prompt, perform the following:
   a. Enter `statuslicense -v` and copy the values for System Identification number (SID) and Module Identification number (MID).
   b. Enter `productid` and copy the value for product ID.

Checking the availability of the FTP, SFTP, or SCP server

Prerequisites

The customer server is accessible over the LAN for backups.

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP (for release 1.x, 2.0 or 2.0.1, the system supports only FTP) server over the customer LAN. You require a current version of the system data to restore the system configuration after you complete the upgrade.

Check with the administrator of the server for the following information about the FTP server:

- Login ID and password
- IP address
- Directory on the FTP server

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

1. Perform one of the following:
   - If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example:
     - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging in from a laptop directly connected to the services port, perform one of the following:
     - If you are using PuTTY configured for SSH, enter `192.11.13.6` in the **Host Name** field and `5022` in the **Port** field.
     - If you are using Telnet, enter `telnet 192.11.13.6 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

   For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.
   Verify that the system displays any filesync errors.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, Avaya recommends that you perform the routine backup for safeguarding the system, in case you need to bring the system to its current configuration.

You can back up the translation files (xln), the system files (os), and the security files on the server to:

- A network device server on the network such as an SCP, SFTP, or FTP server (only FTP server for release 1.x., 2.0 or 2.0.1).
- Flash card using the USB-connected external compact flash drive.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.
   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:

```
Backup successful
```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up files to another server

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, Select **Full Backup** (release-dependent).

   The full backup does not include the datasets for any embedded applications, such as Communication Manager Messaging and SES.
3. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large.
4. Under **Backup Method**, select **Network Device** and select a method from the provided options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
6. Click **Start Backup**.
7. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
8. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:
   Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.

   ii. The system displays the status as the update progresses. The system automatically reboots, if required.

   iii. Click **Yes**.

3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

   ⚠ **Caution:**

   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.
   If you find any announcement sets other than the following, proceed with Step 3:
   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    ```
    Backup successful
    ```

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
   - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.
2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.

4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Upgrade tasks on S8800 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).
- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura ™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:

After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type `service_port_access enable` and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type `ip_forwarding disable` and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:

You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

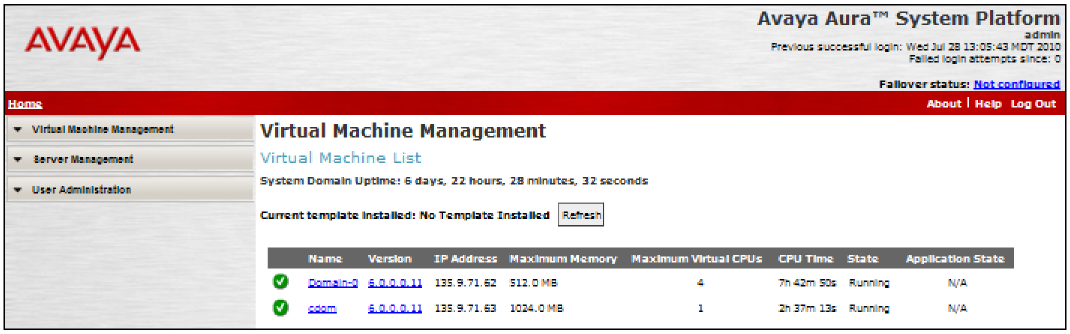
   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



AVAYA
Avaya Aura™ System Platform
admin
Failover status: Not configured
Home
About | Help Log Out
Virtual Machine Management
Server Management
User Administration
Refresh

Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
    - Click **Network Device** and complete the following fields:
        - **Method**
        - **User Name**
        - **Password**
        - **Host Name**
        - **Directory** or **Field Path**
            - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
            - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
    - Click **Local Directory** and provide the path to the backup file on your local directory.

    Important:

    If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
    The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:
   Communication Manager Messaging processes are stopped during RFU installation.

If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.
   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
   a. In the **Name** field, enter `tmp`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
      This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
   a. Record the value of the **Far-end Node Name** field.

      You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
   b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
   a. In the **Name** field, enter `msgserver`.
   b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
   a. In the **Far-end Node Name** field, enter `msgserver`.
   b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.

   Remove the entries from the **Name** and **IP Address** fields and submit the form.

   This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Completion tasks on the S8300 Server

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Turning off the power to the control cabinet

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

   The green light indicates that the cabinet is shut down.

   > **Important:**
   > The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.

2. Remove the power cord from the back of the cabinet.
   The cabinet turns off.

Preupgrade tasks

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. The changing or upgrading the hardware includes:

- Adding the TN2312BP IPSI and TN799D C-LAN circuit packs
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
   - If the information is correct, proceed with Step 3.
   - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

   For more information, see About subnet address.
3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.
4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the cabinet

Installing G650 Media Gateway in the rack

Install G650 Media Gateway in the rack. For instructions, see *Installing the Avaya G650 Media Gateway* (03-300685).

Installing the circuit packs

Addition of circuit packs

Port network (PN) must have an IPSI circuit pack. Add the circuit pack to the PN if it has not already have one.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.

6. Close the IPSI session and log in to the IPSI:
    a. Enter `exit`.

       The system saves the changes and ends the IPSI session.
    b. Enter `192.11.13.6` and log in to the IPSI.
    c. Enter `show control interface`.

       The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
    d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
    a. Enter `exit`.

       The system saves the changes and ends the IPSI session.
    b. Enter `192.11.13.6` and log in to the IPSI.
    c. Enter `show control interface`.

       The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
    d. Enter `reset` and press `Enter`.

       Add or copy the login portion before you add the control gateway.
9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Tasks performed on the new server

Administering the gateway on Communication Manager

Prerequisites

Start a SAT session.

1. Enter `add media-gateway` *`number`*, where *number* is gateway number from 1 to n.

   The system displays the Media Gateway screen.
2. In the **Name** field, enter the hostname assigned to the media gateway.
3. In the **Serial No** field, enter the serial number of the media gateway.

Tip:

To get the serial number, enter `show system` command at the media gateway command line interface.

Caution:

Be sure the serial number for the media gateway you enter in this procedure matches the serial number displayed in the `show system` command. The serial number is case-sensitive, and if entered incorrectly, prevents the server from communicating with the media gateway.

4. In the **Network Region** field, enter the appropriate value.
5. If required, in the **V9** field, enter `gateway-announcements`.

   This field allows you to enable announcements on the media gateway. V9 is a virtual slot. No announcement board is associated the slot. The announcements for the media gateway are available in the media gateway firmware.
6. Press **Enter**.

   If properly administered, the media gateway registers with the main server within 1–2 minutes. The system populates the **IP Address**, **MAC Address**, and **Module Type** fields once the media gateway gets registered with the server.
7. To view the Media Gateway screen, enter `display media-gateway n`, where *n* is the media gateway number.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
    - TN2312BP IPSI
    - TN799DP Control-LAN (C-LAN)
    - TN2302AP or TN2602AP IP Media Processor

    If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface` *`PNnumber`*, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Prerequisites

Start a SAT session.

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:
    - 802.1p: 6
    - DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
    - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.

- To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
  - **802.1p (vlan priority)**: `6`
  - **DiffServ**: `46`
  - **Auto** (port negotiation): `y` for the following default values:
    - `Full duplex`
    - `100mbps` speed
  - **Auto** (port negotiation): `n` to modify as per the network configuration.
    - **Duplex full**
    - **Speed 100**

3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

> **Important:**
> Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:

   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.

6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

   The default is **none**.

Postupgrade tasks on S8800 Server

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay

3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
   - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.

3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.

4. Select where to store or send the backup files:

   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the S8800 Server

Introduction

This section describes the procedure to upgrade the existing S8400 Server running Communication Manager Release 4.0.5 or Release 5.2.1 to Communication Manager Release 6.0.1 on S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.0.1. You reuse the cabinet in the new system.

In this procedure:

- You discard:
    - The TN8400AP or TN8400BP circuit pack
    - The TN8412AP (SIPI) circuit pack
- You retain the following circuit packs:
    - The TN2312 BP IPSI
    - The TN799 DP CLAN
    - The TN2302 or TN2602 Media Processor
- You install the standalone S8800 Server, HP ProLiant DL360 G7 Server, or Dell™ PowerEdge™ R610 Server running System Platform and the simplex main/survivable core template (CM_Simplex).

You install Communication Manager Messaging on the new system because you discard the processor circuit pack that has the Audix feature embedded in it.

The simplex main/survivable core template supports:

- Communication Manager (with or without Communication Manager Messaging)
- Utility Services

The upgrade procedure involves:

- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5 or Release 5.2.1.
- Creating a data set with specific information that you later restore on Communication Manager Release 6.0.1.

- Installing and configuring System Platform and Communication Manager Release 6.0.1 on the new server.
- Installing Communication Manager Messaging (optional).
- Restoring the data set on Communication Manager Release 6.0.1.
- Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.0.1.
- Adding circuit packs to the media gateway.
- Completing the postupgrade administration tasks on Communication Manager Release 6.0.1.

You require a new license for Communication Manager Release 6.0.1.

Use this section to upgrade Communication Manager on:

- The main server
- The survivable core server (formerly enterprise survivable servers)

You can upgrade Communication Manager releases earlier than 4.x to Release 4.0.5 or Release 5.2.1 first before you upgrade to Release 6.0.1. However, this section only mentions upgrading to Release 5.2.1.

Important:

If the existing system is not already on Communication Manager Release 4.0.5 or Release 5.2.1:

- Create a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5 or Release 5.2.1.
- Install Communication Manager Release 4.0.5 or Release 5.2.1 on the S8800 Server and restore the system data from the existing server.
- Continue with the procedures described in this section.

Prerequisites

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that the voice network, dial plan, and E911 for remote locations are redesigned (if needed).	Perform this task only if applicable.

✔	Task	Description
	Verify that you have the required software: • System Platform • the Communication Manager template (as appropriate)	
	Obtain one of the following servers, as appropriate: • S8800 Server • Dell™ PowerEdge™ R610 Server • HP ProLiant DL360 G7 Server	
	Verify that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

Additional documentation needed:

✔	Task	Description
	Installing and Configuring Avaya Aura™ Communication Manager (03-603558)	Provides instructions for installing and configuring Communication Manager.

Preupgrade tasks on the S8400 Server

Connecting to the server

Prerequisites

A CAT5 cross-over cable to connect your services laptop to the server.

1. Plug one end of the CAT5 cross-over cable into the services access port on the server faceplate.
2. Plug the other end of the cross-over cable into the services laptop.
3. Start a SAT session.
4. Log in as `craft`.

Accessing System Management Interface

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

1. Open a compatible Web browser.
2. If you are logging in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.
5. Click **Continue**.
6. Type your password, and click **Logon**.
   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Verifying system status

Verify the groups which are in-service and the groups which are out-of-service before the upgrade.

After you complete the upgrade, compare the postupgrade list with the preupgrade list to ensure that the lists remain the same.

1. Enter `list configuration all`.

   This command displays every circuit pack administered on the system.

2. Enter `list media-gateway`.

   This command displays all H.248 Branch Gateways. Verify that the system registered all required gateways.

3. Enter `list survivable -processor`.

   This command displays the status of registration of the survivable servers and filesync.

4. Enter `list trunk-group`.

   This command displays every trunk group administered on the system.

5. Enter `list hunt-group`.

   This command displays every hunt group administered on the system.

   If any of the command does not complete successfully, escalate the problem immediately. After the upgrade, check the same administration to ensure that the translations are intact.

Clearing alarms

1. Under **Alarms**, select **Current Alarms**.
2. Under **Server Alarms**, select the alarms you want to clear and click **Clear** or **Clear All**.
3. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Prerequisites

Log on to System Management Interface.

1. Under **Security**, click **Server Access**.
2. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**

Starting a SAT session

Prerequisites

If you are using Telnet, enable the Telnet service for Communication Manager.

If Telnet is disabled, use SSH to access the SAT.

Perform one of the following:

- If you are logging on to the corporate LAN, enter the unique IP address of the server in standard dotted-decimal notation. For example, using Telnet, enter `telnet 192.152.254.201 5023`.
- If you are logging on to the server with a laptop that is directly connected to the services port, using Telnet, enter `telnet 192.11.13.6 5023`.

Recording all busyouts

1. Enter `display errors`.
2. In the **Error Type** field, enter `18`.

   The system displays a list of busied out equipment.
3. Record the equipment that is busied out.

Recording node names and IP addresses

1. To get the node names assigned to the TN2302AP IP media processor and TN799C/DP C-LAN circuit packs, enter `display ip-interfaces`.
2. To get the IP addresses that match the node names, enter `list node-names`.
3. Record the information for use after the upgrade.

   After the upgrade, the names and addresses must remain the same.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Disabling scheduled maintenance

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you need to reschedule the daily maintenance activity.

1. Enter `change system-parameters maintenance`.
2. Press **Enter**.
3. Record the settings for the **Stop Time** and **Start Time** fields.
4. Perform one of the following:

- If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
- If scheduled maintenance is not in progress, set the **Start Time** field to a time after the server upgrade is completed.

For example, if you start the server upgrade at 8:00 P.M. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30`.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

You back up the translation files (xln), the system files (os), and the security files on the server to a network device server on the network such as an SCP, SFTP, or FTP server.

If Communication Manager Messaging is enabled on your system, back up the messaging data.

Backing up the files to flashcard

Prerequisites

Log on to System Management Interface (formerly, Maintenance Web interface).

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Full Backup**.
   Full Backup does not backup voice mail configurations or messages.
3. Under **Backup Method**, click **Local PC card**.
4. In the **Retain** field, enter `3`.
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
7. Select the backup from the list and click **Check Status**.
   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Backing up the files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Under **Data Sets**, click **Specify Data Sets** and select the following check boxes:
    - **Avaya Call Processing (ACP) Translations**
    - **Server and System Files**
    - **Security Files**
    - **Communication Manager Messaging (CMM)**

    Select **Translations, Names, and Messages**.
3. Under **Backup Method**, select **Network Device** and select a method from the provided options.
4. Fill in the following fields:
    - **User Name**
    - **Password**
    - **Host Name**, enter the host IP address.
    - **Directory**
5. Click **Start Backup**.
6. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
7. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   ```
   Backup successful
   ```

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Recording configuration information

If you have not already completed, record the current server configuration data that you must configure on the new server. Use the worksheet provided in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341 to record the information.

1. Click **Server Configuration** > **Configure Server**.
2. Click **Continue** on the first and second screen.
3. In the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
4. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
5. Select **Configure Interfaces** and record the following:
    - Server IP address
    - Gateway IP address
    - Subnet mask
    - Integrated Messaging IP address, if configured.
6. Click **Close**.

Copying files to the server

Prerequisites

Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.

Use this procedure to copy the preupgrade service pack or service pack to the server:

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

    Note:
    Do not select the check box, **Install this file on the local server**.
3. Click **Browse** to open the **Choose File** window on your computer.

4. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Install the preupgrade service pack as appropriate for Communication Manager Release 5.2.1 or Release 4.0.5 to prepare the system for upgrade to Release 6.0.1.

1. Under **Server Upgrades**, select **Manage Updates**.
2. Perform one of the following:
   - If the status of the update file you want to activate is packed:
     i. Select the **Update ID** and click **Unpack**.
     ii. Wait until the system displays the message, `... unpacked successfully`.
   - If the status of the update file you want to activate is unpacked:
     i. Select the **Update ID** and click **Activate**.
     ii. The system displays the status as the update progresses. The system automatically reboots, if required.
     iii. Click **Yes**.
3. Click **Continue**.

Backing up Communication Manager

Perform this procedure to generate a backup file that you will restore on the Release 6.0.1 system during the upgrade.

1. Under **Data Backup/Restore**, click **Linux Migration to CM 6.0**.
2. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **User Name**

- **Password**
- **Host Name**
- **Directory**

  The backup location must be a server on the customer LAN.

3. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
4. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
5. Select the backup from the list and click **Check Status**.

   When the backup is complete, the system displays the following message:
   `Backup successful`

   Caution:
   Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Checking for backed up files

Verify that the file `migration-60_*.tar.gz` exists in the location where you backed up the server data.

Here, * is *hostname_hhmmss_YYYYMMDD*. For example, `migration-60_cmhost_012312_20100406.tar.gz`.

Communication Manager Messaging backup

If you are using Communication Manager Messaging, collect optional and custom announcement sets, if you have not already done this before arriving at the site, leave a test message, and shut down Communication Manager Messaging before backing up the files.

You must back up the announcement sets if the customer creates custom announcement sets. You will restore the announcement sets after the upgrade.

Identifying optional announcement sets

If an announcement set appears on the existing system, the announcement set must also be present after an upgrade and before you restore messaging translations. If the announcement set is not present before you restore messaging translations, Communication Manager Messaging does not start successfully. If you installed British English on the existing system, you must restore it after you install Communication Manager on the upgraded system before restoring messaging translations.

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **List Messaging Software**.
3. Note the language packages that the system lists.

   If the system displays any language package other than us-eng and us-tdd, you need to download the additional language packages from a language CD. You will install these language packages on Communication Manager after the upgrade.

Backing up custom announcement sets

Perform this procedure only if Communication Manager Messaging is enabled.

1. Under **Administration**, select **Messaging**.
2. Under **Messaging Administration**, select **Announcement Sets**.

   If you find any announcement sets other than the following, proceed with Step 3:

   - us-eng, us-tdd and us-eng-t
   - Optional announcement set as identified in the Identifying optional announcement sets on page 41 section.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. Under **Data Backup/Restore**, click **Backup Now**.
5. Under **Data Sets**, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. Under **Backup Method**, select **Network Device** and select a method from the provided options.
8. Fill in the following fields:

- **User Name**
- **Password**
- **Host Name**, enter the host IP address.
- **Directory**

9. Click **Start Backup**.
10. Click **Status** to view the backup history.
    The system displays the Backup History page and a list of recent backups.
11. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

    ⚠ **Caution:**

    Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Setting up test data

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and login to the test mailbox.
3. Record a name.
4. Record a greeting and activate the greeting for all calls.
5. Call the test station and record a message.

Shutting down Communication Manager Messaging

1. Perform one of the following:
    - For Communication Manger release earlier than 5.2.1, on the Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.

- For Communication Manger Release 5.2.1 or later, on the **Administration** menu, click **Messaging**.

2. Click **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The shutdown process of the messaging server begins when all users log off from Communication Manager Messaging or after 3 minutes, whichever event is earlier. When this process begins, it takes a few minutes to complete the shutdown. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, click **Specify Data Sets**.
4. Select the **Communication Manager Messaging (CMM)** check box and click **Translations, Names, and Messages**.
5. In the **Download size** field, enter the size of the backed up `.tar` file.

   There could be more than one `.tar` file if the backup size is large when embedded applications, such as Communication Manager Messaging are installed.
6. Under **Backup Method**, select **Network Device** and select a method from the provided options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name**, enter the host IP address.
   - **Directory**
8. Click **Start Backup**.
9. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
10. Select the backup from the list and click **Check Status**.

    When the backup is complete, the system displays the following message:
    `Backup successful`

⚠ **Caution:**

Check the text to verify that there are no error messages. Ignoring the error message can result in files not getting backed up.

Upgrade tasks on S8800 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, the new server is turned on but not connected to the network.

The new server can be one of the following:

- S8800 Server

  For instructions to install, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager* (03-603444).

- Dell™ PowerEdge™ R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

- HP ProLiant DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

Installing System Platform and Communication Manager

Install System Platform, its latest service pack, and the Communication Manager template on the server. For information on the service pack for System Platform that Avaya recommends, see the release notes for Communication Manager available at http://support.avaya.com.

Refer to *Installing and Configuring Avaya Aura ™ Communication Manager* (03-603558) for instructions to install:

- System Platform
- The Communication Manager license
- The Avaya authentication file
- The required Communication Manager template

Important:
After the installation of the Communication Manager template is complete, do not configure Communication Manager, and do not begin to administer Communication Manager translations unless the procedures in this section instruct.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 33.

Important:
You must wait for the first boot process to finish before you can perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

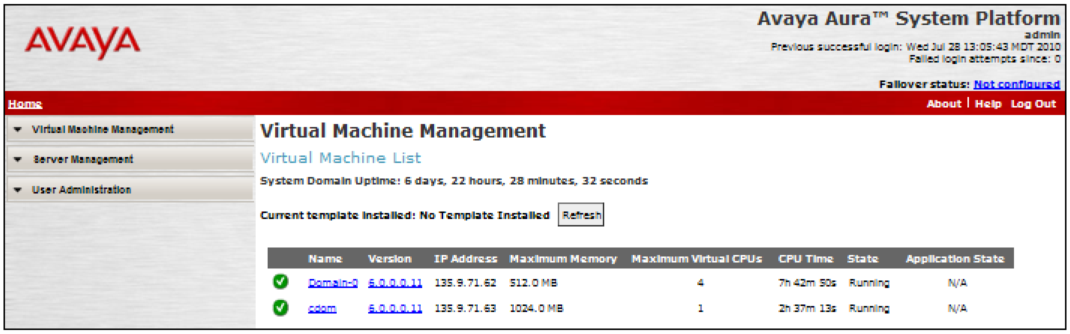
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Verifying the software version

Prerequisites

Log on to the System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Verify the version of the software and the current template installed on the system.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Accessing the System Management Interface

You can access the System Management Interface (SMI) either remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:
   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that is generated by the Logon page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the Communication Manager System Management Interface home page.

Copying files to the server

1. Under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the check box, **Install this file on the local server**.

3. Click **Browse** to open the **Choose File** window on your computer.
4. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.

5. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Restoring the upgrade dataset

Prerequisites

Ensure that the license file is valid.

Note:

You do not need a license file if you are upgrading a survivable core server or survivable remote server.

Install the latest service pack for Communication Manager Release 6.0.1.

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. On the View/Restore page, perform one of the following:
   - Click **Network Device** and complete the following fields:
     - **Method**
     - **User Name**
     - **Password**
     - **Host Name**
     - **Directory** or **Field Path**
       - If you selected `FTP` or `SFTP` in the **Method** field, enter the path to the backup file in the **Directory** field. The system lists the backup files.
       - If you selected `SCP` in the **Method** field, enter the full path of the file in the **File Path** field.
   - Click **Local Directory** and provide the path to the backup file on your local directory.

     Important:

     If the server is not connected to the network, you must select **Local Directory**.
3. Click **View**.
4. Select the files to restore. For example, `migration-60_*.tar.gz` here, * is `hostname_hhmmss_YYYYMMDD`.
5. Click **Restore**.

Configuring server data

Configure the server data using the information provided in the worksheets available in Communication Manager upgrade to simplex and embedded templates - worksheet on page 1341.

On the System Management Interface, under **Server Configuration**, complete the following configurations:

- **Server Role**
- **Network Configuration**

Starting Communication Manager Messaging

Prerequisites

You must have a valid license for Communication Manager.

1. Select **Server** > **Process Status**.
2. Under **Frequency**, select **Display Once**.
3. Click **View**.
4. Ensure that `Messaging` is `UP`. If `Messaging` is not `UP`, start the messaging service:
    a. Select **Miscellaneous** > **Messaging Software**.
    The Messaging Software page displays `Internal messaging is disabled`.
    b. Click **Enable**.
    The Messaging Software page displays the `execution successful...` message at the top of the page and another message that `Internal messaging is enabled`.

Perform the following Communication Manager Messaging procedures only if Communication Manager Messaging is enabled on this system.

Downloading RFU

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the remote field update (RFU):
   - File(s) to download from the machine I'm using to connect to the server.
   - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
   - Click **Browse** to download the RFU.
   - Enter the URL to download the RFU and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.
5. Click **Installed selected packages**.

   Important:
   Communication Manager Messaging processes are stopped during RFU installation.

If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Downloading optional language files

Prerequisites

Language CD.

Perform this task only:

- If the server has Communication Manager Messaging integrated to Communication Manager
- If you identify any optional announcement sets. For instructions, see Identifying optional announcement sets.

1. Insert the language CD-ROM in the CD-ROM drive of your laptop.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Under **Miscellaneous**, click **Download Files**.
4. Select **File(s) to download from the machine I'm using to connect to the server**.
5. Click **Browse** and locate the file to download from the language CD and click **Open**.

   You can select four files at a time from the language CD that you want to copy to the server.
6. Repeat Step 4 to select optional languages and additional languages.
7. Click **Download**.

   The system copies the optional language files and additional languages to the `/var/home/ftp/pub` directory.

   The transfer is complete when the message `Files have been successfully downloaded to the server` appears.

Installing optional announcements

1. Under **Administration**, click **Messaging**.
2. Under **Software Management**, click **Software Install**.
3. Click **Continue without current system backup**.

   The system displays a list of packages available for installation.
4. Select the custom announcement set that you need to install.
5. Click **Install selected packages**.

Restoring custom announcements

Perform this task only if you backed up custom announcement sets. See Backing up custom announcement sets.

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Under **Data Backup/Restore**, click **View/Restore Data**.
3. In the **Method** field, select ftp.
4. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **View**.
6. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
7. Click **Restore**.

Restoring Communication Manager Messaging data

1. Under **Data Backup/Restore**, click **View/Restore Data**.
2. In the **Method** field, select ftp.
3. Enter the following FTP parameters:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**
4. Click **View**.
5. Select the backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
6. Select the backup name and click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Prerequisites

- Obtain the number of the signaling group in use for communication between Communication Manager and Communication Manager Messaging. Use the command `list signaling-group` and search for the signaling group. Typically, the far end node-name for the signaling group is *msgserver*.
- Obtain the IP address of the Communication Manager processor ethernet interface (PROCR) using `status link procr` command.

In Release 6.x, Communication Manager Messaging shares the same IP address as that of Communication Manager. Therefore, you must change the administered signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node-name to support the communication between Communication Manager and Communication Manager Messaging.

1. Enter `change node-names ip tmp`.
    a. In the **Name** field, enter `tmp`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
    This step creates a node name that you will use temporarily.
2. Enter `busyout signaling-group <num>`.
3. Enter `change signaling-group <num>`:
    a. Record the value of the **Far-end Node Name** field.
    You will change this node-name in Step 4. Typically the data in this field is the node-name `msgserver`.
    b. In the **Far-end Node Name** field, enter `tmp` and submit the form.
4. Enter `change node-names ip msgserver`.
    a. In the **Name** field, enter `msgserver`.
    b. In the **IP Address** field, enter `<procr IP addr>` and submit the form.
5. Enter `change signaling-group <num>`.
    a. In the **Far-end Node Name** field, enter `msgserver`.
    b. In the **Far-end Listen Port** field, enter `11720` and submit the form.
6. Enter `release signaling-group <num>`.
7. Enter `change node-names ip tmp`.
    Remove the entries from the **Name** and **IP Address** fields and submit the form.
    This step deletes the temporary node-name.
8. Enter `save translation`.

Configuring the switch link

1. Under Administration, select **Messaging** > **Switch Link Admin.**
2. Under **Signal Group 1**, in the **Messaging TCP** port field, enter `11720`.

Rebooting the server

Prerequisites

Log on to System Platform Web console.

1. Under **Virtual Machine Management**, click **Manage**.
2. Select the name of the system that is running Communication Manager.

   The system opens the Virtual Machine Management - Virtual Machine Detail: cm page.
3. Click **Reboot**.
4. When the system prompts you, click **Yes**.
5. Wait for about 1 minute.
6. On System Management Interface, under **Server**, click **Process Status** to confirm that the reboot is complete.

   Alternatively, you can reboot the server using System Management Interface. To do that:

   a. Under **Server**, click **Shutdown Server**.

   b. Select the **Restart server after shutdown** check box and click **Shutdown**.

Upgrade tasks on the cabinet

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. The changing or upgrading the hardware includes:

- Removing the TN8400AP or TN8400BP and TN8412AP (SIPI) circuit packs from the existing system.
- Connecting the IPSI circuit pack to the customer network
- Assigning static IP address to the IPSI circuit pack

You can perform these tasks while the existing system is in service.

Server and IPSI cable connections

An IPSI circuit pack must have a CAT5 Ethernet cable that connects to the customer network.

Static IP address

You assign static IP address to the IPSI circuit pack. You administer the address directly through the Ethernet port connection on the IPSI faceplate switch which is the top port.

Ensure that you have the IPSI password before you continue with the upgrade.

Completion tasks on the S8400 Server

Shutting down the server

1. Under **Server**, select **Shutdown Server**.
2. Select **Delayed Shutdown**.
3. Clear the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The power-on LED blinks slowly (one flash per second).
5. Wait about 30 seconds.

Disconnecting the laptop from the server

Disconnect the services laptop computer from the server.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
    - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.
    - If you are using Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Administering the Communication Manager system parameters for IPSI

Prerequisites

Start a SAT session.

Administer the IPSI related system parameters on Communication Manager.

1. Enter `change system-parameters ipserver-interface`.
2. Verify the subnet address in the **Primary Control Subnet Address** field:
    - If the information is correct, proceed with Step 3.
    - If the information is incorrect, on the System Management Interface, click **Installation** > **Configure Server** and change the subnet address.

    For more information, see About subnet address.

3. Verify that the **Switch Identifier** field is set correctly for this installation.

   Enter the correct switch identifier in the field before you administer the TN2312 IPSI circuit pack.

4. Verify that the **IPSI Control of Port Networks** field is set to enabled.
5. Press **Enter**.

Tasks performed on the cabinet

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Port network (PN) must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to the PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.
6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.
   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
   d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.
   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

d. Enter `reset` and press `Enter`.

   Add or copy the login portion before you add the control gateway.

9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Turning off the power to the control cabinet

1. On the faceplate of the processor, press and hold the shutdown button until the system starts the shutdown process.

   The green light indicates that the cabinet is shut down.

   Important:

   The latch on the power supply acts as the DC power switch and removes only DC power from the backplane.
2. Remove the power cord from the back of the cabinet.
   The cabinet turns off.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Verifying firmware version

Prerequisites

Log on to System Management Interface.

1. Under **Installation and Upgrades**, click **View IPSI Version**.
2. Select **Query All**, click **View IPSI Version**.
3. Verify the firmware release for the following and any other supported circuit packs:
    - TN2312BP IPSI
    - TN799DP Control-LAN (C-LAN)
    - TN2302AP or TN2602AP IP Media Processor

    If the firmware release does not match with the most current firmware load, you must upgrade the firmware.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing port network circuit packs

Prerequisites

Start a SAT session.

1. Enter `change circuit-pack n`, where n is the cabinet number of the circuit pack.
2. On the Circuit Packs window, go to the carrier and the slot of the circuit pack that you added and leave the field blank.
3. Click **Submit**.

Adding IPSI information

Prerequisites

Start a SAT session.

1. Enter `add ipserver-interface PNnumber`, where *PNnumber* is the port network number.
2. Verify if the **IP Control** field is set to y.
3. If this system has a duplicated bearer network, set the **Administer secondary ip server interface board** field to y.
4. Verify that all the other fields are populated.
5. Press **Enter**.
6. If this system has more than one port network, repeat Step 1 through Step 4 for each port network.

Administering circuit packs

Administering the IPSI circuit pack

Prerequisites

Start a SAT session.

1. Enter `change system-parameters ipserver-interface`.
2. Set the **Switch Identifier** field for the IPSI on this system.
3. Set the QoS parameters:

- 802.1p: 6
- DiffServ: 46

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

Important:
Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Setting the alarm activation level

Prerequisites

Start a SAT session.

1. Enter `change system-parameters maintenance`.
2. In the **CPE Alarm Activation Level** field, select **warning**, **minor**, or **major**, depending on the level that you want.

The default is **none**.

Postupgrade tasks on S8800 Server

Verifying the Communication Manager operation

Performing an integrity check

Prerequisites

Log on to System Management Interface.

1. Under **Server**, click **Status Summary**.
2. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
3. Under **Server**, click **Process Status**.
4. Under **Frequency**, select Display Once.
5. Click **View**.
6. Verify that the system displays `UP SIMPLEX` for all operations.
7. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Prerequisites

- If you are using Telnet, enable the Telnet service for Communication Manager.
- If you are directly connecting the laptop to the services port, enable IP forwarding.

1. Enter the IP address for Communication Manager, for example:
   - If you are using PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- If you are using Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Checking for translation corruption

1. Enter `newterm`.
2. If you see the following message `Warning: Translation corruption detected . . .`, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Enter `list station` and verify that the stations on the new server are the same as the stations that were on the old server.

Checking media modules

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that the server is in operation after the upgrade.

Note:

Skip the sections “Busying out previously busied out equipment” through “Saving translations” if you are upgrading a survivable core server.

Busying out previously busied out equipment

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

1. Enter `change system-parameters maintenance`.
2. Ensure that the administration of **Start Time** and **Stop Time** fields remain the same as what was set before the upgrade.

Saving translations

Prerequisites

Start a SAT session.

Perform the following procedure on the main server only.

1. Enter `save translation all`.
   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays any filesync errors.

Installing the phone message file

Prerequisites

Phone message file, if installed on the existing system, is identified.

If you have to install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

1. Under **Alarms**, click **Current Alarms** to examine the alarm log.
2. If the system lists any alarms, click **Clear** or **Clear All**.
3. Resolve new alarms that have appeared since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up the system

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   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.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Verifying Communication Manager Messaging test data

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify the test name is played.
3. Verify the test message can be played.
4. Call the test station and verify the test greeting is played.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Prerequisites

Network server to back up data.

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select **Communication Manager Messaging (CMM)**.
4. Select **Translations, Names, and Messages**.
5. Select the backup method.
6. Set a password to encrypt the back up data.
7. Type a value from `1` through `200` to limit the size of a transferable file over the network to ensure a successful backup of the Communication Manager Messaging data.

   The specified value in the **Download size** field for the Communication Manager Messaging data being transferred should be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.

8. Click **Start Backup**.

   Communication Manager Messaging downloads and processes each back up file sequentially before downloading the next backup file in the data set.

   Important:

   The backup data set can comprise multiple backup files (tar files). Only the meta tar file (backup file) is visible on the View / Restore Data Web page.

   Note:

   Communication Manager Messaging can restore data from previous releases.

Logging off all administration applications

When you have completed all the administration, log off all the applications used.

Registering the system

Use the standard procedure to register the system.

Appendix A: Communication Manager upgrade to simplex and embedded templates - worksheet

Use this worksheet to record the information from the Communication Manager Release 5.2.1 server. Use the completed worksheet to configure the Communication Manager Release 6.0.x server on simplex survivable core template, simplex survivable remote template, embedded survivable core template, or embedded survivable remote template.

When you restore the upgrade dataset, you will observe the following on the Server Role Web page:

- The system automatically populates the following information:
    - **Server role**
    - **SID**
    - **MID**
    - **Memory Setting**
    - **Media Gateway serial number**
- You must manually enter the values in other fields, using this worksheet.

Note:

IPv6 is restricted therefore, you need to keep it disabled unless you are instructed to enable it. If IPv6 is disabled, do not enter the information in the IPv6 fields.

Server Role

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Role	MAIN, ESS or LSP	**Configure Server > Server Role**	
SID		`statuslicense -v`	RFA System ID
MID		`statuslicense -v`	RFA Module ID
Registration address		**Configure Server > Configure LSP/ESS**	

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Registration address IPv6		Does not exist in Release 5.2.1	
File Synch address		**Configure Server > Configure LSP/ESS**	
File Synch address		**Configure Server > Configure LSP/ESS**	If MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	
File Synch address IPv6		Does not exist in Release 5.2.1	If MAIN is duplicated
File Synch address		**Configure Server > Configure LSP/ESS**	Optional
File Synch address		**Configure Server > Configure LSP/ESS**	Optional, if MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	Optional
File Synch address IPv6		Does not exist in Release 5.2.1	Optional, if MAIN is duplicated
This server's memory setting	Small, Medium or Large		The system populates with upgrade dataset restore. Also, see Help on Server Role Web page.
Media gateway serial number		Does not exist in Release 5.2.1	See, HELP on Server Role Web page on Release 6.0.x.

Network Configuration

When you restore the upgrade dataset, you will observe the following on the Network Configuration Web page:

- The system automatically populates the following information:
    - **eth0 functional assignment**
    - **Server ID**
- If a field is blank after the restore, manually enter the data using this worksheet.

The system automatically populates **Host Name**, **Gateway and Mask** and **IP addresses** fields from the System Platform settings.

Enter the values in the **DNS Domain**, **Domain Search List,** and **DNS** fields either on Communication Manager interface or on **Server Management** > **Network Configuration** page of the System Platform Web console. Entering on the System Platform Web console is the preferred method.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server > Set Identities**	View only, populated during the installation of System Platform
DNS Domain		**Configure Server > DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates this field in Communication Manager • As simple hostname, you can configure this field in Communication Manager
Search Domain list 1		**Configure Server > DNS**	In Communication Manager Release 6.0.x, **Domain Search list** is a single field and accepts comma separated values. Combine the values obtained from **Search Domain list 1** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager Release 6.0.x. If **Domain Search list** is configured on System Platform, the **Domain Search list** field is automatically populated in Communication Manager. If **Domain Search list** is not configured on System Platform, you can configure the **Domain**

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Search list in Communication Manager.
Search Domain list 2		**Configure Server > DNS**	
Search Domain list 3		**Configure Server > DNS**	
Search Domain list 4		**Configure Server > DNS**	
Search Domain list 5		**Configure Server > DNS**	
Primary DNS		**Configure Server > DNS**	Entered on System Platform at the time of installation
Secondary DNS		**Configure Server > DNS**	Entered on System Platform at the time of installation
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.
Server ID		**ID** field on Status Summary page	
Default Gateway		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of System Platform
eth0 IP address IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of Communication Manager template.
eth0 mask IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of Communication Manager template.
eth0 IP address IPv6		Does not exist in Release 5.2.1	View only, populated during the installation of

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Communication Manager template.
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	

Appendix B: Communication Manager upgrade to duplex template - worksheet

Use this worksheet to record the information from the Communication Manager Release 5.2.1 server. You must use the completed worksheet to configure the Communication Manager Release 6.0.x server on duplex main/survivable template.

When you restore the upgrade dataset, you observe the following on the Server Role Web page:

- The system automatically populates the following information:
  - **Server role**
  - **SID**
  - **MID**
  - **Memory Setting**
- You must manually enter the values in other fields, using this worksheet.

Note:

IPv6 is restricted therefore, you need to keep it disabled unless you are instructed to enable it. If IPv6 is disabled, do not enter the information in the IPv6 fields.

Server Role

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Role	MAIN or ESS	**Configure Server > Server Role**	
SID		`statuslicense -v`	RFA System ID
MID		`statuslicense -v`	RFA Module ID
Only for survivable core (ESS) server			
Registration address		**Configure Server > Configure ESS**	
Registration address IPv6		Does not exist in Release 5.2.1	
File Synch address		**Configure Server > Configure ESS**	

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
File Synch address		**Configure Server > Configure ESS**	If MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	
File Synch address IPv6		Does not exist in Release 5.2.1	if MAIN is duplicated
File Synch address		**Configure Server > Configure ESS**	Optional
File Synch address		**Configure Server > Configure ESS**	Optional, if MAIN is duplicated
File Synch address IPv6		Does not exist in Release 5.2.1	Optional
File Synch address IPv6		Does not exist in Release 5.2.1	Optional, if MAIN is duplicated
This server's memory setting	Small, Medium or Large		Auto populates with upgrade dataset restore. Also, see Help on Server Role Web page.

Network Configuration

Server 1

When you restore the upgrade dataset, you will observe the following changes on the Network Configuration Web page:

- The system automatically populates the following information:
  - **eth0 functional assignment**
  - **Server ID**
- If a field is blank after the restore, manually enter the data using this worksheet.

The system automatically populates **Host Name**, **Gateway and Mask** and **IP addresses** from the System Platform settings.

Enter the values in the **DNS Domain**, **Domain Search List,** and **DNS** fields either on Communication Manager interface or on **Server Management** > **Network Configuration** on the System Platform Web console. Entering on the System Platform Web console is the preferred method.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server > Identities**	View only, populated during the installation of System Platform

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Alias Host Name		**Configure Server > Identities**	
DNS Domain		**Configure Server > DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates this field in Communication Manager • As simple hostname, you can configure this field in Communication Manager
Search Domain list 1		**Configure Server > DNS**	In Communication Manager Release 6.0.x, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Search Domain list 1** to **Search Domain list 5** fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager Release 6.0.x. If **Domain Search List** is configured on System Platform, the **Domain Search List** field is automatically populated in Communication Manager. If **Search Domain list 1** is not configured on System Platform, you can configure the **Search Domain list 1** in

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Communication Manager.
Search Domain list 2		**Configure Server > DNS**	
Search Domain list 3		**Configure Server > DNS**	
Search Domain list 4		**Configure Server > DNS**	
Search Domain list 5		**Configure Server > DNS**	
Primary DNS		**Configure Server > DNS**	Entered on System Platform at the time of installation
Secondary DNS		**Configure Server > DNS**	Entered on System Platform at the time of installation
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.
Server ID		**ID** field on Status Summary page	
Default Gateway		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of System Platform
Default Gateway IPv6		Does not exist in Release 5.2.1	

Table 2: etho

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth0 IP address IPv4		**Configure Server > Set Identities** and	View only, populated during the installation of

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
		Configure Server > Configure Interfaces	Communication Manager template.
eth0 mask IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of Communication Manager template.
eth0 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of Communication Manager template.
eth0 Alias IP address		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	For MAIN, you can choose to make the Processor Ethernet available.

Table 3: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an Ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server > Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server > Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of Communication Manager template.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 Alias IP address	Leave this field blank	Not applicable	Leave this field blank
eth1 functional assignment	select **Duplication Link**	Not applicable	Select **Duplication Link**

Duplication Parameters

Table 4: Server 1

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Duplication	Encrypted or un-Encrypted	**Configure Server > Set Identities**	See the worksheets for **Network Configuration**
Hostname		**Configure Server > Set Identities**	Enter the hostname of the other server
Server ID		**Configure Server > Set Identities**	Enter the server ID of the other server
Corporate LAN/PE IP address		**Configure Server > Configure Interfaces**	Enter the eth0 IP address of the other server
Corporate LAN/PE IP address IPv6		Does not exist in Release 5.2.1	Enter the eth0 IP (IPv6) address of the other server
Duplication IP address		**Configure Server > Configure Interfaces**	Enter the eth1 IP address of the other server
Duplication IP address, IPv6		Does not exist in Release 5.2.1	Enter the eth1 IP (IPv6) address of the other server
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	**Configure Server > Configure Interfaces**	Must be the same for both servers
IP address for PE Healthcheck		**Configure Server > Configure Interfaces**	
IP address for PE Healthcheck IPv6		Does not exist in Release 5.2.1	

Network Configuration

Server 2

When you restore the upgrade dataset, you will observe the following changes on the Network Configuration Web page:

- The system automatically populates the following information:
  - **eth0 functional assignment**
  - **Server ID**
- If a field is blank after the restore, manually enter the data using this worksheet.

The system automatically populates **Host Name**, **Gateway and Mask** and **IP addresses** from the System Platform settings.

Enter the values in the **DNS Domain**, **Domain Search List,** and **DNS** fields either on Communication Manager interface or on **Server Management** > **Network Configuration** on the System Platform Web console. Entering on the System Platform Web console is the preferred method.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server > Identities**	View only, populated during the installation of System Platform
Alias Host Name		**Configure Server > Identities**	
DNS domain		**Configure Server > DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates thisCommunication Manager • as simple hostname, you can configure this field in Communication Manager
Search Domain list 1		**Configure Server > DNS**	In Communication Manager Release 6.0.x, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Domain Search List** to **Search**

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Domain list 5 fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager Release 6.0.x. If **Domain Search List** is configured on System Platform, the **Domain Search List** field is automatically populated in Communication Manager. If **Search Domain list 1** is not configured on System Platform, you can configure the **Search Domain list 1** in Communication Manager.
Search Domain list 2		**Configure Server > DNS**	
Search Domain list 3		**Configure Server > DNS**	
Search Domain list 4		**Configure Server > DNS**	
Search Domain list 5		**Configure Server > DNS**	
Primary DNS		**Configure Server > DNS**	Enter these values on the System Platform Web console
Secondary DNS		**Configure Server > DNS**	Enter these values on the System Platform Web console
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.
Server ID		**Status Summary > ID**	

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Default Gateway		**Configure Server > Set Identities**	View only, populated during the installation of System Platform
Default Gateway IPv6		Does not exist in Release 5.2.1	

Table 5: eth0

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Note
eth0 IP address IPv4		**Configure Server > Configure Interfaces**	View only, populates during the installation of Communication Manager template.
eth0 mask IPv4		**Configure Server > Configure Interfaces**	View only, populates during the installation of Communication Manager template.
eth0 IP address, IPv6		Does not exist in Release 5.2.1	If present, populates during the installation of Communication Manager template.
eth0 Alias IP address		**Configure Server > Configure Interfaces**	
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	For main, you can choose to make the Processor Ethernet available.

Table 6: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server > Configure Interfaces**	This field is the Duplication Interface IP address for this server.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server > Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of Communication Manager template.
eth1 Alias IP address	Leave this field blank	**Configure Server > Configure Interfaces**	Leave this field blank
eth1 functional assignment	select **Duplication Link**	**Configure Server > Set Identities**	Select **Duplication Link**

Duplication Parameters

Table 7: Server 2

Field	Value	Method for obtaining from 5.2.1	Notes
Server Duplication	Encrypted or un-Encrypted	**Configure Server > Set Identities**	See the worksheets for **Network Configuration**
Hostname		**Configure Server > Set Identities**	Enter the hostname of the other server
Server ID		**Configure Server > Set Identities**	Enter the server ID of the other server
Corporate LAN/PE IP address		**Configure Server > Configure Interfaces**	Enter the eth0 IP address of the other server
Corporate LAN/PE IP address IPv6		Does not exist in Release 5.2.1	Enter the eth0 IP (IPv6) address of the other server
Duplication IP address		**Configure Server > Configure Interfaces**	Enter the eth1 IP address of the other server

Field	Value	Method for obtaining from 5.2.1	Notes
Duplication IP address, IPv6		Does not exist in Release 5.2.1	Enter the eth1 IP (IPv6) address of the other server
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	**Configure Server > Configure Interfaces**	Must be the same for both servers
IP address for PE Healthcheck		**Configure Server > Configure Interfaces**	
IP address for PE Healthcheck IPv6		Does not exist in Release 5.2.1	

Appendix C: Communication Manager upgrade simplex to duplex template - worksheet

Use this worksheet to record the information from a simplex server running Communication Manager Release 5.2.1. You must use the completed worksheet to configure the Communication Manager Release 6.0.x server on duplex main/survivable core template.

When you restore the upgrade dataset, on the Server Role Web page, the system:

- Automatically populates the following information:
    - **Server role**
    - **SID**
    - **MID**
    - **Memory Setting**
- Displays some blank fields, where you enter the values, using this worksheet.

✱ **Note:**
IPv6 is restricted therefore, keep it disabled unless you are instructed to enable it. If IPv6 is disabled, do not enter the information in the IPv6 fields.

Server Role

Server 1 and Server 2

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Server Role	MAIN or ESS	**Configure Server > Server Role**	
SID		`statuslicense -v`	RFA System ID
MID		`statuslicense -v`	RFA Module ID
This server's memory setting	Small, Medium, or Large		Auto populates with upgrade dataset restore. Also, see Help on Server Role Web page.
Only for survivable core (ESS) server			

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Registration address		**Configure Server > Configure ESS**	
Registration address IPv6		Does not exist in Release 5.2.1	
File Synch address Main		**Configure Server > Configure ESS**	
File Synch address Main duplicate		**Configure Server > Configure ESS**	If MAIN is duplicated
File Synch address IPv6 Main		Does not exist in Release 5.2.1	
File Synch address IPv6 Main duplicate		Does not exist in Release 5.2.1	if MAIN is duplicated
File Synch address Alternate		**Configure Server > Configure ESS**	Optional
File Synch address Alternate duplicate		**Configure Server > Configure ESS**	Optional, if Alternate is duplicated
File Synch address IPv6 Alternate		Does not exist in Release 5.2.1	Optional
File Synch address IPv6 Alternate duplicate		Does not exist in Release 5.2.1	Optional, if Alternate is duplicated

Network Configuration

Server 1

You are required to assign a unique server ID to both the servers. The original simplex server has a server ID assigned to it. You can assign the same server ID to one of the new server pair. For example, if the server ID of the original simplex server is 1, you can assign *1* to one server and *2* to the other server.

For duplicated survivable core server (formerly, ESS), the server ID on the Network Configuration Web page must also correspond to Communication Manager translations on the corresponding survivable-processor SAT screen. See *Avaya Aura™ CommunicationManager Survivability Options* (03-603633) for more information on administering Communication Manager for survivable processors.

When you restore the upgrade dataset, you observe the following changes on the Network Configuration Web page:

- The system automatically populates the following information:
    - **eth0 functional assignment**
    - **Server ID**
- If a field is blank after the restore, enter the data using this worksheet.

The system automatically populates **Host Name**, **Gateway and Mask** and **IP addresses** from the System Platform settings.

Enter the values in the **DNS Domain**, **Domain Search List,** and **DNS** fields either on Communication Manager interface or on **Server Management** > **Network Configuration** on the System Platform Web console. Entering on the System Platform Web console is the preferred method.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server > Identities**	View only, populated during the installation of System Platform. The hostname will be a new name specific to server 1 of the new pair of servers. Do not use the hostname of the Communication Manager Release 5.2.1 server. You use Release 5.2.1 hostname in another field.
Alias Host Name		**Configure Server > Identities**	Use the hostname of the Communication Manager Release 5.2.1 server.
DNS Domain		**Configure Server > DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates this field in Communication Manager • As simple hostname, you can configure this field in Communication Manager
Search Domain list 1		**Configure Server > DNS**	In Communication Manager Release 6.0.x, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Search Domain list 1** to **Search Domain list 5**

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager Release 6.0.x. If **Domain Search List** is configured on System Platform, the **Domain Search List** field is automatically populated in Communication Manager. If **Search Domain list 1** is not configured on System Platform, you can configure the **Search Domain list 1** in Communication Manager.
Search Domain list 2		**Configure Server > DNS**	
Search Domain list 3		**Configure Server > DNS**	
Search Domain list 4		**Configure Server > DNS**	
Search Domain list 5		**Configure Server > DNS**	
Primary DNS		**Configure Server > DNS**	Entered on System Platform at the time of installation
Secondary DNS		**Configure Server > DNS**	Entered on System Platform at the time of installation
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.
Server ID		**ID** field on Status Summary page	

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Default Gateway		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of System Platform
Default Gateway IPv6		Does not exist in Release 5.2.1	

Table 8: eth0

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth0 IP address IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of Communication Manager template. Use the IP address assigned for server 1. Do not use the IP address of the Communication Manager Release 5.2.1 server. This IP address will be used in another field.
eth0 mask IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	View only, populated during the installation of Communication Manager template.
eth0 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of Communication Manager template.
eth0 Alias IP address IPv4		**Configure Server > Set Identities** and **Configure Server > Configure Interfaces**	Use the IP address of the Communication Manager Release 5.2.1 server.
eth0 Alias IP address IPv6		Does not exist in Release 5.2.1	

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	For MAIN, you can choose to make the Processor Ethernet available.

Table 9: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an Ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server > Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server > Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of Communication Manager template.
eth1 Alias IP address	Leave this field blank	Not applicable	Leave this field blank
eth1 functional assignment	select **Duplication Link**	Not applicable	Select **Duplication Link**

Duplication Parameters

Table 10: Server 1

Field	Value	Notes
Server Duplication	Encrypted or un-Encrypted	See the worksheets for **Network Configuration**
Hostname		Enter the hostname of the other server
Server ID		Enter the server ID of the other server

Field	Value	Notes
Corporate LAN/PE IP address		Enter the eth0 IP address of the other server
Corporate LAN/PE IP address IPv6		Enter the eth0 IP (IPv6) address of the other server
Duplication IP address	192.11.13.14	Enter the eth1 IP address of the other server
Duplication IP address, IPv6		Enter the eth1 IP (IPv6) address of the other server
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	Must be the same for both servers
IP address for PE Healthcheck		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see HELP on the Duplication Parameters web page.
IP address for PE Healthcheck IPv6		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see HELP on the Duplication Parameters web page.

Network Configuration

Server 2

You are required to assign a unique server ID to both the servers. The original simplex server has a server ID assigned to it. You can assign the same server ID to one of the new server pair. For example, if the server ID of the original simplex server is 1, you can assign *1* to one server and *2* to the other server.

For duplicated survivable core server (formerly, ESS), the server ID on the Network Configuration Web page must also correspond to Communication Manager translations on the corresponding survivable-processor SAT screen. See *Avaya Aura™ CommunicationManager Survivability Options* (03-603633) for more information on administering Communication Manager for survivable processors.

When you restore the upgrade dataset, you will observe the following changes on the Network Configuration Web page:

- The system automatically populates the following information:
  - **eth0 functional assignment**
  - **Server ID**
- If a field is blank after the restore, enter the data using this worksheet.

The system automatically populates the values for **Host Name**, **Gateway and Mask** and **IP addresses** from the System Platform settings.

Enter the values in the **DNS Domain**, **Domain Search List,** and **DNS** fields either on Communication Manager interface or on **Server Management** > **Network Configuration** on the System Platform Web console. Avaya recommends you to enter the values on the System Platform Web console.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Host Name		**Configure Server > Identities**	View only, populated during the installation of System Platform. The hostname will be a new name specific to server 1 of the new pair of servers. Do not use the hostname of the Communication Manager Release 5.2.1 server. This will be used in another field.
Alias Host Name		**Configure Server > Identities**	Use the exact hostname of the Communication Manager Release 5.2.1 server.
DNS domain		**Configure Server > DNS**	If you have configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates thisCommunication Manager • as simple hostname, you can configure this field in Communication Manager
Search Domain list 1		**Configure Server > DNS**	In Communication Manager Release 6.0.x, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Domain Search List** to **Search**

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Domain list 5 fields from Communication Manager Release 5.2.1 into a single comma separated list for Communication Manager Release 6.0.x. If **Domain Search List** is configured on System Platform, the **Domain Search List** field is automatically populated in Communication Manager. If **Search Domain list 1** is not configured on System Platform, you can configure the **Search Domain list 1** in Communication Manager.
Search Domain list 2		**Configure Server > DNS**	
Search Domain list 3		**Configure Server > DNS**	
Search Domain list 4		**Configure Server > DNS**	
Search Domain list 5		**Configure Server > DNS**	
Primary DNS		**Configure Server > DNS**	Enter these values on the System Platform Web console
Secondary DNS		**Configure Server > DNS**	Enter these values on the System Platform Web console
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values, it does not automatically populate the third DNS value.
Server ID		**Status Summary > ID**	

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Default Gateway		**Configure Server > Set Identities**	View only, populated during the installation of System Platform
Default Gateway IPv6		Does not exist in Release 5.2.1	

Table 11: eth0

eth0 represents the IP interface for Corporate LAN, Control Network or Processor Ethernet functionality. On the existing Communication Manager Release 5.2.1 server, the Corporate LAN, Control Network, and Processor Ethernet may have been assigned to an ethernet interface other than eth0.

Field	Value	Method for obtaining from CM Release 5.2.1	Note
eth0 IP address IPv4		**Configure Server > Configure Interfaces**	View only, populates during the installation of Communication Manager template. Use the IP address assigned for server 1. Do not use the IP address of the Communication Manager Release 5.2.1 server. This IP address will be used in another field.
eth0 mask IPv4		**Configure Server > Configure Interfaces**	View only, populates during the installation of Communication Manager template.
eth0 IP address, IPv6		Does not exist in Release 5.2.1	If present, populates during the installation of Communication Manager template.
eth0 Alias IP address IPv4		**Configure Server > Configure Interfaces**	Use the IP address of the Communication Manager Release 5.2.1 server.
eth0 Alias IP address IPv6		Does not exist in Release 5.2.1	
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	For main, you can choose to make the

Field	Value	Method for obtaining from CM Release 5.2.1	Note
			Processor Ethernet available.

Table 12: eth1

eth1 represents the IP interface for duplication functionality of Communication Manager. On the existing Communication Manager 5.2.1 server, the Duplication Interface may have been assigned to an ethernet interface other than eth1.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
eth1 IP address IPv4		**Configure Server > Configure Interfaces**	This field is the Duplication Interface IP address for this server. Typically: • 192.11.13.13 for server 1 • 192.11.13.14 for server 2
eth1 mask IPv4		**Configure Server > Configure Interfaces**	Typically 255.255.255.252.
eth1 IP address IPv6		Does not exist in Release 5.2.1	If present, populated during the installation of Communication Manager template.
eth1 Alias IP address	Leave this field blank	**Configure Server > Configure Interfaces**	Leave this field blank
eth1 functional assignment	select **Duplication Link**	**Configure Server > Set Identities**	Select **Duplication Link**

Duplication Parameters

Table 13: Server 2

Field	Value	Notes
Server Duplication	Encrypted or un-Encrypted	See the worksheets for **Network Configuration**
Hostname		Enter the hostname of the other server
Server ID		Enter the server ID of the other server

Field	Value	Notes
Corporate LAN/PE IP address		Enter the eth0 IP address of the other server
Corporate LAN/PE IP address IPv6		Enter the eth0 IP (IPv6) address of the other server
Duplication IP address	192.11.13.13	Enter the eth1 IP address of the other server
Duplication IP address, IPv6		Enter the eth1 IP (IPv6) address of the other server
PE Interchange Priority	HIGH, EQUAL, LOW, or IGNORE	Must be the same for both servers
IP address for PE Healthcheck		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see HELP on the Duplication Parameters web page.
IP address for PE Healthcheck IPv6		The network gateway router is the default address. You can also use the IP address of other device on the network that responds. For more information, see HELP on the Duplication Parameters web page.

Appendix D: Converting private control networks A and B to control network C

Introduction

Before you upgrade the system to Communication Manager Release 6.0.x, you must remove private control networks, and place all IPSI on the network that connects the Communication Manager server to the corporate LAN.

This procedure applies to duplicated Communication Manager servers with the following conditions:

- Servers that are not yet upgraded to Communication Manager Release 6.0.x.
- Port networks with duplicated IPSI circuit pack (S8700-series servers, S8800, Dell™ PowerEdge™ R610, or HP ProLiant DL360 G7 Servers in duplex configuration).
- Port networks with simplex IPSI circuit pack.

Preparing for port network conversion

1. Collect the location of all IPSI circuit packs in control network A (CN-A) and control network B (CN-B).
2. On a worksheet, assign a new public (static) control network IP addresses to each CN-A and CN-B IPSI in the system.
3. Verify that all port networks have duplicated IPSI circuit packs.

   This activity determines whether the changes impacts the service. Duplicate IPSIs infer the changes may be executed on each circuit pack as the IPSI is in standby mode.

Note:

If an IPSI contains only one IPSI (not duplicated IPSI, which may be the case for some port networks), the conversion to CN-C affects the service for that port network.

4. Assign a port to the network switches supporting the IPSIs to connect to the public network routing system.
5. Obtain required cables for connecting the switch. Do not use the cables from the former dedicated (private) control network.

Converting private control network to control network C

Prerequisites

- IPSIs are running the latest available firmware.
- DHCP service for private control networks is disabled on Communication Manager servers.
- SAT session is started.

Convert the duplicated IPSI systems on the public control network to control network C.

1. Connect the network switch devices, supporting the IPSIs, to customer (public) control network.

   Note:

   Do not disconnect the Ethernet switch private network from the Communication Manager servers until instructed.

2. If a public network is not assigned to the server community:
   a. Logon to the server.
   b. Enter `cnc on`.

      Execute this command on:

      - Both Communication Manager servers.
      - Any survivable core servers that are part of the system.
3. Enter `set ipserver-interface b-all`.

4. Enter `list ip-server-interface` to confirm that all b-side boards are active.

   If all b-side boards are not active, interchange the boards individually and debug issues until the b-side boards in all port networks are in-service.

5. Enter `change ipserver-interface X`.
   a. In the **Secondary IPSI** field, enter the new IP addresses.
   b. Continue to change all b-side IPSI addresses.
   c. When all b-side IPSIs are successfully changed, enter `list ipserver-interface` command and confirm that all b-side IPSIs are in service. Because the network switch is connected to the public network, the IPSIs show `0.0.0.0`, indicating that all aspects of connectivity are good

6. When all b-side IPSIs are in service, enter `set ipserver-interface a-all` to interchange the IPSIs.

   All a-side IPSIs must be in standby and in service, debug the IPSIs if they are not active.

7. Repeat the address changes for all a-side IPSIs.

8. Enter `list ipserver-interface` and verify that all IPSI interfaces display `0.0.0.0`.

9. Enter `list sys-link` and verify that the associated EAL links are up (data taken from a different maintenance interface than the previous command).

10. Place some IP and TDM type calls and exercise a couple of IPSI interchanges to confirm reliability.

11. Change the management IP addresses of the CN-A and CN-B Ethernet switches to an available address in the newly connected public control network.
    a. On Ethernet switches, reboot to make this new address active. To prevent loss of service, reboot only when the respective set of IPSIs are in standby mode.
    b. Disconnect and remove Ethernet cables from CN-A and CN-B ports of the server and the former CN-A and CN-B switches.

Appendix E: Converting from fiber port networks to IP-PNC

Overview

Fiber port network connectivity (fiber-PNC) uses the circuit-switched (TDM) protocol to transport bearer traffic (voice, fax, video) between port networks (PN) over fiber-optic cables. IP-PNC uses the packet-switched Internet Protocol to transport bearer traffic over Ethernet cables.

Note:

The term fiber-PNC used in this document has almost the same meaning as the term multiconnect. Multiconnect implies a dedicated control network and fiber-PNC that carry the bearer traffic. The term fiber-PNC applies to configurations with a dedicated or a nondedicated control network.

You are required to change the MCC1, SCC1, and G650 cabinets present in the current fiber-PNC configuration to IP-PNC configuration.

When you convert a system to IP-PNC, the **Internet Protocol (IP) PNC** field on the Customer Options screen is set to y.

The conversion procedures apply to individual PNs in a communications system that is composed of one or more PNs. In the final converted system, the PNs are 100% IP-PNC.

Use these procedures to convert the fiber-PNC to IP-PNC. These procedures are applicable for PNs controlled by servers running Communication Manager Release 3.0 and later.

Fiber-PNC configurations

The conversion procedures cover the following three fiber-PNC configurations:

- Direct connect

In this configuration, one PN, the control PN, is IPSI-connected to the control network, and one or two additional PNs are fiber-connected to the control PN. The fiber connections are between the TN570 Expansion Interface (EI) circuit packs in the PNs.

- Center Stage Switch (CSS)

  In this configuration, all PNs are fiber-connected through the CSS and one or more PNs are connected to the control network through the TN2312 IP Server Interface (IPSI) circuit pack. The fiber connections are between the TN573 Switch Node Interface (SNI) circuit packs and the TN570 Expansion Interface (EI) circuit packs. The SNI circuit packs reside in a switch node carrier. The EI circuit packs reside in a PN. The fiber also can connect SNIs in two switch-node carriers.

- Asynchronous Transmission Mode (ATM)

  In this configuration, all PNs are fiber-connected through the ATM switch, and one or more PNs are connected to the control network through the TN2312 IP Server Interface (IPSI) circuit pack. The fiber connections are between the ATM switch and the TN2305B or TN2306B ATM Interface circuit packs in the PNs.

The starting configuration

The starting configuration consists:

- Two or three fiber-PNC PNs in a direct connect configuration
- Up to 64 fiber-PNC PNs that use CSS or an ATM switch

All PNs are fiber-connected, and one or more PNs are IPSI-connected to the control network. For Communication Manager release 3.0 and later, the starting configuration may include some IP-PNC components in addition to the fiber-PNC components. Each PN may be implemented in an MCC1, an SCC1 stack, or a G650 stack. The overall system may be any combination of MCC1, SCC1, or G650 Media Gateways.

The starting configuration can be any of the following:

- Simplex or duplex servers
- Simplex or duplex control networks
- Simplex or duplex bearer networks

The converted configuration

The final converted configuration is all IP-PNC. Fiber-PNC does not exist after the conversion.

The final configuration can only be on port networks controlled by a server running Communication Manager on a simplex or a duplex template.

For systems that are controlled by a server running a simplex or a duplex template, the IP-PNC components can have a simplex or a duplex control networks and a simplex or a duplex bearer network.

Prerequisites

Preconversion checklist

Before you start the conversion, ensure that you have the conversion specific hardware:

✔	Task	Description
	Obtain the following circuit packs: • TN2312BP IPSI • TN2302AP HW11 (or later) or TN2602AP Media Processor • TN799DP C-LAN	

Conversion tasks checklist

Conversion procedure involves the following major tasks:

#	Task
1	Changing synchronization
2	Adding new circuit packs
3	Upgrading firmware on circuit packs
4	Disabling PNC duplication
5	Removing fiber-related administration
6	Enabling PNC duplication
7	Removing fiber-related hardware

#	Task
8	Administering PN synchronization
9	Completing post-conversion tasks

Changing synchronization

Use this procedure only if you are converting the PN that contains the direct-connect, CSS or ATM synchronization source. Perform the following steps to remove or change the synchronization source:

Synchronization for a direct connect configuration is derived from a fiber-PNC. Synchronization for the ATM is derived from a connection through an ATM-connected PN.

1. Perform one of the following:
    - For direct connect and CSS, enter `change synchronization css`.
    - For ATM, enter `change synchronization atm`.
2. Leave the **Primary** and **Secondary** fields blank.
3. Click **Submit**.
4. Verify that the synchronization sources are updated correctly.
5. Enter `list synchronization`.
6. Verify that the **Primary** field and the **Secondary** field are blank.

Installing the circuit packs

Addition of circuit packs

You replace the processor circuit pack with a TN2312BP IPSI circuit pack.

Each port network must have an IPSI circuit pack and at least one media processor circuit pack. Add these circuit packs to each PN that does not already have them. The media processor circuit packs can be TN2602AP or TN2302AP Media Processor. The TN2602AP circuit pack provides higher capacities and allows for duplication of the bearer network.

You may install additional media processors to increase the capacity. However, you cannot install more than two TN2602AP circuit packs in a PN. The need for additional media processor circuit pack depends on the configuration parameters of the system such as number of IP endpoints.

Depending on the system configuration, you may need additional TN799DP C-LAN circuit packs. You require TN799DP, if the system supports IP endpoints, H.248 Branch Gateways, or other IP adjuncts. The number of C-LAN circuit packs you need depends on the system parameters such as the number of IP endpoints and the desired level of availability.

Installing a circuit pack

1. Insert the circuit pack into the appropriate slot.
2. Push firmly on the faceplate until the circuit pack is properly seated and close the latch.

Connecting to the server

1. Connect one end of the CAT5 straight-through cable to the IPSI adapter on the back of the cabinet or the gateway.
2. Connect the other end of the cable to the Ethernet switch on the customer network.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.

4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.

5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.

6. Close the IPSI session and log in to the IPSI:

   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.

   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.

7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.

8. Close the IPSI session and log in to the IPSI:

   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.

   b. Enter `192.11.13.6` and log in to the IPSI.

   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.

9. Enter `exit`.

Verifying the installation of the circuit pack

Prerequisites

Start a SAT session.

1. Enter `display circuit-pack` *`cabinetnumber`* to open the Circuit Packs window.
2. Verify that the circuit packs you installed are shown in the appropriate slots.

Connecting the cables

Cables for the new circuit packs

The IPSI, Media processor and the C-LAN circuit packs are connected to the customer LAN.

Each of the three types of circuit packs requires an I/O adapter that is connected to the backplane amphenol connector. The adapters for the three types of circuit packs are different and not necessarily interchangeable. Also, the adapters for the TN2302AP and TN2602AP media processor circuit packs are different. Ensure that you use the correct adapter that corresponds to each type of circuit pack, for example, if you use TN2602, ensure that you use a TN2602 adapter.

Connecting the circuit pack cables

1. Connect the I/O adapter of the circuit pack to the backplane amphenol connector that corresponds to the slot in which you installed the circuit pack.
2. Connect a CAT5 or better Ethernet cable to the top RJ45 jack on the I/O adapter of the circuit pack.

   This jack is labeled **Port 1**.
3. Connect the other end of the CAT5 cable to an RJ45 jack on the customer LAN.

Administering circuit packs

Administration of the new circuit packs

In addition to the administration procedures described in this section, you might also need to adjust the administration of the network regions. Your planning documents might provide information about changes to network regions. For more information on how to administer network regions, see *Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504*.

Tip:

To avoid the loss of new translations, save translations frequently during the administration process.

Administering the IPSI circuit packs

Prerequisites

Start a SAT session.

Complete Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

1. If any of the IPSIs in the configuration are duplicated, enter `change system-parameters duplication` to set the **Enable Operation of IPSI Duplication** field to `y`.
2. Enter `change system-parameters ipserver-interface` to set:
   - The **Switch Identifier** field for the IPSIs on this system:
     - If the identifier is A, proceed with the next step.
     - If the identifier is not A, enter the correct value between B to J in the **Switch Identifier** field and click **Submit**.
   - The QoS parameters:
     - 802.1p: 6

- DiffServ: 46

3. To add a new IPSI, enter `add ipserver-interface n`, where n is the PN number.

Configuring the IPSI circuit pack

For static addressing, perform the steps on the circuit pack:

1. Connect the services laptop to the Services port on the IPSI faceplate.
2. Enter `telnet 192.11.13.6` to access the IPSI.
3. At the prompt, enter `ipsilogin` to log in to the IPSI IP Administration Utility.
4. Log in as `craft` and enter the IPSI password.

   The default IPSI password is serv1ce.
5. To configure the static IP address and the netmask, enter `set control interface` *`ipaddr netmask`*.
6. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.
   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.
   d. Enter `reset` and press `Enter`.
7. If the IPSI uses a default gateway, enter `set control gateway` *`gatewayaddr`*, where gatewayaddr is the customer-provided IP address for the network gateway.
8. Close the IPSI session and log in to the IPSI:
   a. Enter `exit`.

      The system saves the changes and ends the IPSI session.
   b. Enter `192.11.13.6` and log in to the IPSI.
   c. Enter `show control interface`.

      The system displays the IP address, the subnet mask, and the default gateway information. Verify that the information displayed is correct.

   d. Enter `reset` and press `Enter`.

      Add or copy the login portion before you add the control gateway.

9. Enter `exit`.

Setting the VLAN parameters and diffserv parameters

Prerequisites

Start a SAT session.

1. Enter `add ipserver interface`.
2. Perform one of the following:
   - For the system to take the values set in `change system parameters ipserver interface`, set the **Use System Level Parameter Values?** field to `yes`.
   - To set the qos parameters for an IPSI, set the **Use System Level Parameter Values?** field to `no` and complete the following parameters:
     - **802.1p (vlan priority)**: `6`
     - **DiffServ**: `46`
     - **Auto** (port negotiation): `y` for the following default values:
       - `Full duplex`
       - `100mbps` speed
     - **Auto** (port negotiation): `n` to modify as per the network configuration.
       - **Duplex full**
       - **Speed 100**
3. To check the administered values, enter `show qos`.
4. To end the IPSI session, enter `exit`.

   Important:

   Ensure that the IPSI port settings and the Ethernet port settings are the same. A mismatch between the two causes data loss. Ensure that the port settings on the Ethernet switches are the same as those appear in the **`set port`** commands.

Verifying IPSI translations

1. Enter `list ipserver-interface`.
2. Verify that the IPSI circuit packs are translated.

   The **State of Health - C P E G** column shows `0.0.0.0` for each healthy IPSI. If the column shows `1` in any position, troubleshoot the problem.

   The pattern `0.1.1.0` usually means that a cabinet type is administered incorrectly or a connectivity problem exists, such as an incorrectly terminated cable.

Verifying IPSI connectivity

Prerequisites

Log on to System Management Interface.

1. Under **Diagnostics**, click **Ping**.
2. Under **Endpoints to Ping**, select **IPSIs with cab number (1–99) ___ carrier number ___**.
3. Enter the correct gateway numbers in the text boxes.
4. Click **Execute Ping**.
5. Verify that the endpoints respond correctly.

Administering the media processor circuit pack

Prerequisites

Start a SAT session.

Use this procedure to administer TN2602AP and TN2302AP Media Processor circuit packs.

If you are administering the media processor circuit pack on a duplicated server, log on to the active server.

1. To verify that the TN2602AP is correctly registered in the installed location, enter `list configuration board UUCSS`.
2. Verify the firmware version in the **Vintage** column. If the version is earlier than the latest version that is available on the Avaya Support Web site, upgrade the TN2602AP firmware.
3. To verify the number of TN2602AP VoIP channels, enter `display system-parameters customer-options`, and go to page 2.
4. In the **Maximum TN2602AP VoIP Channels** field, verify the number of TN2602 circuit packs with 80 VoIP channels and the number of TN2602 circuit packs with 320 VoIP channels.
5. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN2602APs.
6. For each new TN2602AP circuit pack, enter `add ip-interface UUCSS` to open the IP Interfaces screen and complete each field with the information for this circuit pack.

   Note:

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
7. To test the connectivity to the IP endpoints through each TN2602AP, enter `ping ip-address ipadress board UUCSS`, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN2602AP. *UUCSS* is the cabinet, carrier, and slot location of the TN2602AP.
8. Repeat step 7 for another IP endpoint on a different subnet.
9. Make an external trunk call to a telephone on the port network and leave the call active.
10. To verify call processing, enter `status media-processor board UUCSS`.
11. Review the **LINKS** and **DSP CHANNEL STATUS** categories to determine whether the call is being processed.

Administering the C-LAN circuit pack

1. To verify that the TN799DP is correctly registered in the installed location, enter `list configuration board UUCSS`, where *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
2. Verify the firmware version in the **Vintage** column.

   If the version is earlier than the latest version that is available on the Avaya Support web site, you must upgrade the TN799DP firmware.
3. To open the IP Node Names window, enter `change node-names ip` and enter the node names and the IP addresses for the TN799DPs.
4. For each new TN799DP circuit pack:
   a. Enter `add ip-interface` *`UUCSS`* to open the IP Interfaces screen.
   b. Complete each field with the information for this circuit pack.

   If you do not have a gateway IP address, leave the **Gateway Address** field blank.
5. To display the Data Module window:
   a. Enter `add data-module next`.
   b. In the **Type** field, enter `ethernet`.
   c. Complete the remaining fields on the window.
6. To test connectivity to the IP endpoints through each TN799DP, enter `ping ip-address` *`ipadress`* `board` *`UUCSS`*, where *ipaddress* is the IP address of an IP endpoint that is on the same subnetwork as the TN799DP. *UUCSS* is the cabinet, carrier, and slot location of the TN799DP.
7. Repeat Step 6 for another IP endpoint on a different subnet.

Firmware upgrade on the new circuit packs

The IPSI, the media processor, and the C-LAN circuit packs that you add must have the latest available firmware installed. Check the version of the firmware that is installed on each circuit pack and compare with the latest version that is available on the Avaya Support Web site. If a circuit pack does not have the latest version installed, upgrade the firmware on the circuit pack.

If you have not already copied the latest firmware to your laptop, download the latest firmware files from the Avaya Support Web site available at http://avaya.com/support.

Upgrading IPSI firmware

Each IPSI circuit pack must be on the latest and same firmware version. You can obtain the latest version of the firmware from Avaya Support Site available at http://avaya.com/support. However, use the latest firmware installed to the utility server. For more information, see *Accessing and Managing Utility Server* (03-603628).

Download the latest firmware to TN2312BP IPSI circuit pack.

The process requires IP connectivity to the IPSIs.

For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* from the Avaya Support Web site.

Removing fiber-related administration

Prerequisites

Start a SAT session.

Before you can use the IP connections, remove the fiber administration for each fiber-connected PN. Perform this procedure to busyout and remove the fiber links for each PN.

1. To view the fiber link numbers and the endpoints, enter `list fiber-link`.
2. Enter `busyout fiber-link` *n*, where *n* is the link number for the fiber connection.
3. Enter `remove fiber-link` *n*.
4. Repeat Step 2 and Step 3 for each IP-PNC PN.

Disabling PNC duplication

If the bearer network is duplicated, remove the duplication before you remove the fiber-optic connections. If the system does not have PNC duplication, continue with the next procedure.

1. To check which of the duplicated PNCs is active, enter `status pnc`.
2. To busyout the standby PNC, enter `busyout pnc-standby`.
3. To open the duplication screen, enter `change system-parameters duplication`.
4. In the **Enable Operation of PNC Duplication** field, enter `n` and click **Submit**.

Removing fiber-related hardware

Complete these steps for each PN that you are converting to IP-PNC:

1. Remove the fiber cables that connect the following circuit packs in the PNs:
   - For direct connect and CSS configuration, expansion interface (EI) circuit packs and TN570
   - For ATM configuration, ATM EI circuit packs and TN2305B or TN2306B
2. For ATM configuration, remove the DS1 cable connecting the ATM switch to the sync splitter, if present.
3. Remove the circuit packs from the cabinets, carriers, or gateways in the PNs.

Administering PN synchronization

Prerequisites

Open a SAT session.

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

1. To view the synchronization information for the IP-PNC PNs, enter `list synchronization` and `status synchronization`.
2. Verify that the following fields are blank:
   - The **Primary** and the **Secondary** fields on the Synchronization Plan window.
   - The **Source Physical Location** field on the Synchronization Status window.
3. Enter `change synchronization port-network` *n*, where *n* is the PN number of the converted port network that requires synchronization.
4. Enter `list cabinet`.

   The system displays a list of all the cabinets and the PNs that the cabinets contain under **Circuit Packs Available for Synchronization**.
5. Obtain a location for the synchronization source circuit pack from the list under **Circuit Packs Available for Synchronization** for **Primary** and **Secondary** fields. Ensure that you choose a working synchronization source.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, add another synchronization-source circuit pack location in the **Secondary** field.
8. Press **Submit**.

   Wait about 5 minutes for Communication Manager to update the synchronization plan.
9. To verify the changes, enter `list synchronization` and the `status synchronization` commands.
10. If the **Switching Capability** field for this PN is disabled on the Synchronization Status window, enter `enable synchronization-switch all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must show `PASS` in the **Results** field. If the **Results** field does not show `PASS`, you must troubleshoot the synchronization error.

Index