Upgrading to Avaya Aura® Communication Manager

Release 6.2
03-603560
Issue 1.0
December 2012

© 2012 Avaya Inc.

All Rights Reserved.

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

Warranty

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

Licenses

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

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

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, 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.
- Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

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 and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction 15
- Purpose 15
- Intended audience 15
- Related resources 15
  - Documentation 16
  - Training 19
  - Avaya Mentor videos 19
- Support 20
- Warranty 20
- Communication Manager upgrades 20
- System Platform 21
- Communication Manager templates overview 22
- Supported platform for survivable servers 24
- License file for Communication Manager 25
- Duplicated server licensing 26
- Authentication files for Communication Manager 26
- Use of third-party certificates 27
- Upgrade paths 27
- Support for SIP Enablement Services 28
- Special circumstances 28
- Preupgrade requirements 29
- Upgrade order 30
- Upgrade process 30
- Required documents 34
- Using the Upgrading to Communication Manager book 35

Chapter 2: Upgrading from Release 6.0.x to Release 6.2.1 37
- Upgrading from Release 6.0.x to 6.2.1 on simplex template 37
  - Introduction 37
  - Preupgrade tasks 38
  - Prerequisites 39
  - Preupgrade tasks on the existing system 39
  - Upgrade tasks 51
- Upgrading from Release 6.0.x to 6.2.1 on duplex template 63
  - Introduction 63
  - Preupgrade tasks 64
  - Prerequisites 65
  - Preupgrade tasks on the active server 65
  - Preupgrade tasks on the standby server 74
  - Upgrade tasks on the standby server that was active before the interchange 87
  - Postupgrade tasks on the active server running Release 6.2.1 95
  - Postupgrade tasks on the standby server running Release 6.2.1 101
- Upgrading from Release 6.0.x to 6.2.1 on embedded main template 105
  - Introduction 105
  - Presite upgrade checklist 106

Preupgrade tasks on the existing system ... 107
Upgrade tasks ... 118
Chapter 3: Upgrading to simplex main/survivable template ... 133
Upgrading the S8500A Server to the HP DL360 G7 or Dell R610 Server ... 133
Introduction ... 133
Preupgrade tasks on the S8500A Server ... 134
... 0
Upgrade tasks on a new server that supports Release 4.0.5 ... 148
Upgrade tasks on the HP DL360 G7 or Dell R610 (Release 6.2) Server ... 161
Postupgrade tasks on the HP DL360 G7 or Dell R610 (Release 6.2) Server ... 169
Upgrading the S8500-Series Server to the HP DL360 G7 or Dell R610 Server ... 176
Introduction ... 176
Preupgrade tasks ... 177
Prerequisites ... 178
Upgrade tasks on the target server ... 194
Upgrading the S8510 Server to S8510 Server on System Platform ... 214
Introduction ... 214
Preupgrade tasks ... 215
Prerequisites ... 215
Upgrade tasks ... 237
Upgrading the S8800 Server to S8800 Server on System Platform ... 256
Introduction ... 256
Preupgrade tasks ... 257
Prerequisites ... 259
Upgrade tasks ... 283
Upgrading the S8800 Server to the HP DL360 G7 or Dell R610 Server ... 304
Introduction ... 304
Preupgrade tasks ... 305
Prerequisites ... 306
Upgrade tasks on the target server ... 322
Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform ... 342
Introduction ... 342
Preupgrade tasks ... 342
Prerequisites ... 343
Upgrade tasks ... 359
Upgrading DEFINITY SI or R Server to the HP DL360 G7 or Dell R610 Server ... 379
Introduction ... 379
Prerequisites ... 381
Preupgrade tasks ... 382
Preupgrade administration ... 384
Upgrade tasks ... 386
Postupgrade tasks on the new server ... 411
Chapter 4: Upgrading to simplex survivable remote template ... 419
Upgrading the S8500A Server to the HP DL360 G7 or Dell R610 Server ... 419
Introduction ... 419
Preupgrade tasks on the S8500A Server ... 420
Upgrade tasks on the Release 6.2.1 Server ... 425

Upgrading the S8500-Series Server to the HP DL360 G7 or Dell R610 Server ... 435
Introduction ... 435
Preupgrade tasks ... 436
Prerequisites ... 438
Upgrade tasks on the HP DL360 G7 or Dell R610 Server ... 449
Upgrading the S8510 Server to S8510 Server on System Platform ... 461
Introduction ... 461
Preupgrade tasks ... 462
Prerequisites ... 463
Upgrade tasks ... 478
Upgrading the S8800 Server to S8800 Server on System Platform ... 490
Introduction ... 490
Preupgrade tasks ... 491
Prerequisites ... 493
Upgrade tasks ... 511
Upgrading the S8800 Server to the HP DL360 G7 or Dell R610 Server ... 524
Introduction ... 524
Preupgrade tasks ... 524
Prerequisites ... 526
Upgrade tasks on the HP DL360 G7 or Dell R610 Server ... 537
Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform ... 549
Introduction ... 549
Preupgrade tasks ... 550
Prerequisites ... 550
Upgrade tasks ... 563
Upgrading DEFINITY SI or R Server to the HP DL360 G7 or Dell R610 Server ... 575
Introduction ... 575
Prerequisites ... 576
Preupgrade tasks ... 577
Preupgrade administration ... 579
Upgrade tasks ... 581
Postupgrade tasks on the new server ... 600
Chapter 5: Upgrading to duplex main/survivable core template ... 605
Upgrading the S8500A Server to the HP DL360 G7 or Dell R610 Server ... 605
Introduction ... 605
Preupgrade tasks ... 606
Prerequisites ... 607
Preupgrade tasks on the S8500A Server ... 608
... 0
Upgrade tasks on a new server that supports Release 4.0.5 ... 623
... 0
Upgrade tasks on the HP DL360 G7 or Dell R610 (Release 6.2.1) Server ... 635
Completion tasks on the active S8500A Server ... 644
Postupgrade tasks on the first HP DL360 G7 or Dell R610 (Release 6.2.1) active server ... 645
Upgrade tasks on the second HP DL360 G7 or Dell R610 Server ... 652
Upgrading the S8500B or S8500C Server to HP DL360 G7 or Dell R610 Server ... 665
Introduction ... 665

Presite preparation 666
Preupgrade tasks on the S8500B or S8500C Server 667
Installing the servers in the rack 678
Duplex main/survivable core template 678
Upgrade tasks on the first HP DL360 G7 or Dell R610 Server 678
Upgrade tasks on the second HP DL360 G7 or Dell R610 Server 694
Upgrading the S8510 server to the HP DL360 G7 or Dell R610 Server 707
Introduction 707
Presite preparation 708
Preupgrade tasks on the S8510 Server 710
Installing the servers in the rack 720
Duplex main/survivable core template 720
Upgrade tasks on the first HP DL360 G7 or Dell R610 Server 720
Upgrade tasks on the second HP DL360 G7 or Dell R610 Server 736
Upgrading the S8700-Series Servers to the HP DL360 G7 or Dell R610 Servers 749
Introduction 749
Presite preparation 751
Preupgrade tasks on the active S8700 Server 752
Preupgrade tasks on the standby S8700 Server 766
Preparing the new servers for the upgrade 777
..... 0
Staging the new servers to Communication Manager Release 5.2.1 777
Upgrade tasks on the first staged (Release 5.2.1) server 788
Upgrade tasks on the second staged (Release 5.2.1) Server 792
Upgrade tasks on the first staged (Release 5.2.1) Server 796
Completion tasks on both the staged (Release 5.2.1) servers 800
Upgrade tasks on both the new (Release 6.2.1) servers 804
Verification tasks on the staged servers running Release 6.2.1 813
Verification tasks on the first staged active (Release 6.2.1) server 814
Completion tasks on the standby S8700 Server 815
Completion tasks on the active S8700 Server 818
Postupgrade tasks on the first staged Release 6.2.1 active server 820
Postupgrade tasks on the second staged Release 6.2.1 server (busied out) 827
Upgrading the S8700-Series servers to the HP DL360 G7 or Dell R610 Servers 832
Introduction 832
Presite preparation 833
Preupgrade tasks 834
Preupgrade tasks on the active S8700-Series Server 835
Preupgrade tasks on the standby S8700-Series Server 846
Installing the servers in the rack 855
Upgrade tasks on the first HP DL360 G7 or Dell R610 Server 855
Upgrade tasks on the second HP DL360 G7 or Dell R610 Server 871
Upgrading the S8800 Server to S8800 Server on System Platform 884
Introduction 884
Presite preparation 885
Preupgrade tasks 886
Preupgrade tasks on the active S8800 Server 888

Preupgrade tasks on the standby S8800 Server ... 898
Tasks on the active S8800 server ... 924
Upgrade tasks on the standby server ... 925
Upgrade tasks on the S8800 Server that is shutdown ... 927
Postupgrade tasks on the standby server ... 952
Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform ... 958
Introduction ... 958
Preupgrade tasks ... 958
Upgrading branch gateways and survivable servers ... 959
Survivable core servers resetting ... 960
Preupgrade tasks on the active HP DL360 G7 Server ... 960
Preupgrade tasks on the standby HP DL360 G7 Server ... 970
Tasks on the active HP DL360 G7 Server ... 986
Upgrade tasks on the standby server ... 987
Upgrade tasks on the server that is shutdown ... 989
Postupgrade tasks on the standby server ... 1004
Upgrading the S8800 Server to HP DL360 G7 or Dell R610 Server ... 1010
Introduction ... 1010
Presite preparation ... 1011
Preupgrade tasks on the active S8800 Server ... 1012
Preupgrade tasks on the standby S8800 Server ... 1022
Installing the servers in the rack ... 1030
Duplex main/survivable core template ... 1030
Upgrade tasks on the first HP DL360 G7 or Dell R610 Server ... 1030
Upgrade tasks on the second HP DL360 G7 or Dell R610 Server ... 1046
Upgrading DEFINITY SI or R Server to the HP DL360 G7 or Dell R610 Server ... 1059
Introduction ... 1059
Prerequisites ... 1060
Preupgrade tasks ... 1061
Preupgrade administration ... 1063
Upgrade tasks on both the new servers ... 1065
Verification tasls on the HP DL360 G7 or Dell R610 Servers ... 1073
Tasks on the first HP DL360 G7 or Dell R610 Server ... 1075
Postupgrade administration on both the servers ... 1076
Postupgrade tasks on the first HP DL360 G7 or Dell R610 Server ... 1092
Postupgrade tasks on the second HP DL360 G7 or Dell R610 Server ... 1098
Chapter 6: Upgrading to embedded main template ... 1103
Upgrading DEFINITY SI or CSI Server to the S8300D Server ... 1103
Introduction ... 1103
Prerequisites ... 1104
Preupgrade tasks ... 1105
Preupgrade administration ... 1106
Upgrade tasks ... 1108
Postupgrade tasks on S8300D Server ... 1125
Upgrading the S8300A Server to S8300D Server ... 1131
Introduction ... 1131
Checking the FTP, SFTP, or SCP server information ... 1132

Preupgrade tasks on the S8300 Server 1132
Upgrade tasks on the S8300D (Release 4.0.1 or 5.2.1) Server 1147
Upgrade tasks on the S8300D (Release 6.2.1) Server 1159
Upgrading the S8300 Server to the S8300D Server 1179
Introduction 1179
Upgrade paths 1180
Required upgrade sequence 1180
Onsite preparation 1181
Upgrade tasks on the S8300D Server 1196
Upgrading S8400 Server to the S8300D Server 1217
Introduction 1217
Prerequisites 1218
Preupgrade tasks on the S8400 Server 1219
Upgrade tasks on the S8300D Server 1233
Postupgrade tasks on S8300D Server 1249
Completion tasks on the S8400 Server 1256
Upgrading S8500 Server to the S8300D Server 1257
Introduction 1257
Prerequisites 1258
Preupgrade tasks on S8500 Server 1260
Upgrade tasks on the S8300D Server 1275
Completion tasks on S8500 Server 1291
Postupgrade tasks on S8300D Server 1292
Upgrading the S8300D Server to S8300D Server on System Platform 1299
Introduction 1299
Preupgrade tasks on S8300 Server 1300
Upgrade tasks on the S8300D Server 1315
Chapter 7: Upgrading to embedded survivable remote template 1337
Upgrading DEFINITY SI or CSI Server to the S8300D Server 1337
Introduction 1337
Prerequisites 1338
Preupgrade tasks 1339
Preupgrade administration 1340
Upgrade tasks 1341
Postupgrade tasks on S8300D Server 1351
Upgrading the S8300A Server to S8300D Server 1357
Introduction 1357
Prerequisites 1357
Upgrade tasks on the S8300D Server 1366
Upgrading the S8300 Server to S8300D Server 1377
Introduction 1377
Onsite preparation 1378
Upgrade tasks on the S8300D Server 1390
Upgrading S8400 Server to the S8300D Server 1402
Introduction 1402
Prerequisites 1403
Preupgrade tasks on the S8400 Server 1405

Upgrade tasks on the S8300D Server ... 1408
Postupgrade tasks on S8300D Server ... 1415
Completion tasks on the S8400 Server ... 1420
Upgrading S8500 Server to the S8300D Server ... 1421
Introduction ... 1421
Prerequisites ... 1423
Preupgrade tasks on the S8500 Server ... 1424
Upgrade tasks on the S8300D Server ... 1428
Postupgrade tasks on S8300D Server ... 1435
Completion tasks on S8500 Server ... 1440
Upgrading the S8300D Server to S8300D Server on System Platform ... 1441
Introduction ... 1441
Preupgrade tasks on S8300 Server ... 1442
Upgrade tasks on the S8300D Server ... 1452
Chapter 8: Converting to port network ... 1465
Upgrading DEFINITY Server CSI in CMC to the HP DL360 G7 or Dell R610 Server ... 1465
Introduction ... 1465
Prerequisites ... 1466
Preupgrade tasks ... 1467
Preupgrade administration ... 1469
Upgrade tasks ... 1471
Postupgrade tasks on HP DL360 G7 or Dell R610 Server ... 1493
Upgrading DEFINITY ONE/S8100 in CMC to the HP DL360 G7 or Dell R610 Server ... 1498
Introduction ... 1498
Prerequisites ... 1499
Preupgrade tasks ... 1500
Preupgrade administration ... 1502
Upgrade tasks ... 1504
Postupgrade administration ... 1516
Postupgrade tasks on HP DL360 G7 or Dell R610 Server ... 1526
Upgrading Avaya IP600/S8100 Server in G600 to the HP DL360 G7 or Dell R610 Server ... 1531
Introduction ... 1531
Prerequisites ... 1532
Preupgrade tasks ... 1534
Preupgrade administration ... 1535
Upgrade tasks ... 1538
Postupgrade administration ... 1550
Postupgrade tasks on HP DL360 G7 or Dell R610 Server ... 1560
Upgrading S8300 Server to the HP DL360 G7 or Dell R610 Server ... 1565
Introduction ... 1565
Prerequisites ... 1567
Preupgrade tasks on the S8300 Server ... 1568
Upgrade tasks on HP DL360 G7 or Dell R610 Server ... 1582
Shutting down the S8300 Server ... 1596
Preupgrade tasks ... 1597
Postupgrade administration ... 1598
Postupgrade tasks on the HP DL360 G7 or Dell R610 Server ... 1606

Upgrading S8400 Server to the HP DL360 G7 or Dell R610 Server ... 1613
Introduction ... 1613
Prerequisites ... 1614
Preupgrade tasks on the S8400 Server ... 1615
Upgrade tasks on HP DL360 G7 or Dell R610 Server ... 1628
Upgrade tasks on the cabinet ... 1642
Completion tasks on the S8400 Server ... 1643
Postupgrade administration ... 1643
Postupgrade tasks on the HP DL360 G7 or Dell R610 Server ... 1653
Appendix A: Worksheet for upgrading Communication Manager to simplex and embedded templates ... 1661
Appendix B: Worksheet for upgrading Communication Manager to duplex template 1667
Appendix C: Worksheet for upgrading Communication Manager on simplex to duplex template ... 1679
Appendix D: Converting private control networks A and B to control network C ... 1693
Introduction ... 1693
Preparing for port network conversion ... 1693
Converting private control network to control network C ... 1694
Appendix E: Converting from fiber port networks to IP-PNC ... 1697
Overview ... 1697
Fiber-PNC configurations ... 1697
The starting configuration ... 1698
The converted configuration ... 1698
Prerequisites ... 1699
Preconversion checklist ... 1699
Conversion tasks checklist ... 1699
Changing synchronization ... 1700
Installing the circuit packs ... 1700
Addition of circuit packs ... 1700
Installing a circuit pack ... 1701
Connecting to the server ... 1701
Configuring the IPSI circuit pack ... 1701
Verifying the installation of the circuit pack ... 1702
Connecting the cables ... 1703
Cables for the new circuit packs ... 1703
Connecting the circuit pack cables ... 1703
Administering circuit packs ... 1703
Administration of the new circuit packs ... 1703
Administering the IPSI circuit pack ... 1704
Configuring the IPSI circuit pack ... 1704
Setting the VLAN parameters and diffserv parameters ... 1705
Verifying IPSI translations ... 1706
Verifying IPSI connectivity ... 1707
Administering the media processor circuit pack ... 1707
Administering the C-LAN circuit pack ... 1708
Firmware upgrade on the new circuit packs ... 1709
Upgrading IPSI firmware ... 1709

Removing fiber-related administration..... 1710
Disabling PNC duplication..... 1710
Removing fiber-related hardware..... 1711
Administering PN synchronization..... 1711
Index..... 1713

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Communication Manager from earlier releases to Release 6.2.1 on System Platform. The document includes upgrade checklist, upgrade, and verification procedures for each supported upgrade path.

Intended audience

The primary audience for this document is anyone who is involved with upgrading, maintaining, and verifying Communication Manager on System Platform at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Related resources

Note:

For information about the screens referenced in this book, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

The following documents provide additional information.

- *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504
- *ATM Installation, Upgrades, and Administration using Avaya Communication Manager*, 555-233-124
- *Avaya Application Solutions: IP Telephony Deployment Guid*e, 555-245-600
- *Avaya Business Advocate User Guide*, 07-300653
- *Avaya Aura® Call Center 5.2 Automatic Call Distribution (ACD) Reference*, 07-602568
- *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent selection (EAS) Reference*, 07-600780

- *Avaya Communication Manager Advanced Administration Quick Reference*, 03-300364
- *Avaya Communication Manager Basic Administration Quick Reference*, 03-300363
- *Avaya Communication Manager Basic Diagnostics Quick Reference*, 03-300365
- *Avaya Remote Feature Activation (RFA) User Guide*, 03-300149
- *Avaya Toll Fraud and Security Handbook*, 555-025-600
- *Converged Communications Server Installation and Administration*, 555-245-705
- *DEFINITY Communications Systems Generic 2.2 and Generic 3 Version 2 DS1/CEPT1/ ISDN PRI Reference*, 555-025-107
- *DEFINITY Enterprise Communications Server Release 1.1 Getting Started with the Avaya R300 Remote Office Communicator*, 555-233-769
- *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205
- *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207
- *Installation, Upgrades and Additions for Avaya CMC1 Media Gateways*, 555-233-118
- *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300430
- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431
- *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300432
- *Avaya Aura® Communication Manager Overview*, 03-300468
- *Avaya Aura® Communication Manager Reports*, 555-233-505
- *Avaya Aura® Communication Manager Screen Reference*, 03-602878
- *Avaya Aura® Communication Manager System Capacities Table*, 03-300511
- *Avaya Aura® Communication Manager Survivable Options*, 03-603633
- *What's New in Avaya Aura® Communication Manager, Avaya Servers and Branch Gateways for Release 6.0*, 03-601528

For documents not listed here, see http://www.avaya.com. Select **Support** and then **Product Documentation**.

Related topics:

Documentation on page 16
Training on page 19
Avaya Mentor videos on page 19

Documentation

To successfully complete the upgrade, you must refer to more books. The following table provides a reference to the specific book you must use to perform that part of the

Communication Manager upgrade. Download the documents from the Avaya Support website at http://support.avaya.com.

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 you can upgrade directly.	*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 you cannot upgrade directly.	*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 6.2*, 03-603560 (this book)	
Complete the routine preupgrade tasks on the existing server.	*Upgrading to Avaya Aura® Communication Manager Release 6.2*, 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 6.2*, 03-603560 (this book)	
Install the preupgrade service pack on the existing server.	*Upgrading to Avaya Aura® Communication Manager Release 6.2*, 03-603560 (this book)	
Back up all the data sets to be restored on the new server.	*Upgrading to Avaya Aura® Communication Manager*	

Task	Book to use	Notes
	Release 6.2, 03-603560 (this book)	
Install the server in the rack.	Use one of the following books as appropriate: • *Installing the HP ProLiant DL360 G7 Server*, 03-603799 • *Installing the Dell™ PowerEdge™ R610 Server*, 03-603793	
Install the S8300D 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 appropriate book for your 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	
(Optional) Install postupgrade service pack.	*Upgrading to Avaya Aura® Communication Manager Release 6.2*, 03-603560 (this book)	
Restore the datasets on the new server	*Upgrading to Avaya Aura® Communication Manager Release 6.2*, 03-603560 (this book)	

Task	Book to use	Notes
Configure Communication Manager through the System Management Interface.	*Upgrading to Avaya Aura® Communication Manager Release 6.2*, 03-603560 (this book)	Use this book to configure Communication Manager.
Complete the postupgrade administration.	*Upgrading to Avaya Aura® Communication Manager Release 6.2*, 03-603560 (this book)	

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. To search for a course, log in to the Avaya Learning Center, enter the course code in the **Search** field, and click **Go**.

Course code	Course title	Type
ATI02348VEN	Avaya Aura® Communication Manager Implementation	Web Base Course
4U001151	Avaya Aura® Communication Manager Implementation Upgrade (R5.x to R6.x)	Instructor Let Course
4U00115V	Avaya Aura® Communication ManagerImplementation Upgrade (R5.x to R6.x)	Virtual Course
1M00211W	Avaya Aura® Communication Server 1000 Upgrade Essentials	Web Base Course

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Support

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

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

Communication Manager upgrades

This book provides the process and procedures for upgrading Avaya Aura® Communication Manager to Release 6.2.1. 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.x or Release 6.2 to Release 6.2.1.
- Hardware and software upgrade: Replacing the existing server with the server that Communication Manager Release 6.2.1 supports.
  - For systems on Release 5.2.1, upgrading from Release 5.2.1 to Release 6.2.1.
  - For systems on Release 4.0.5, upgrading from Release 4.0.5 to Release 6.2.1.
  - 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 6.2.1

- 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 6.2.1

You can upgrade Communication Manager from Release 5.2.1 or Release 6.0.x to Release 6.2.1 on the following servers:

- Avaya S8300D Server
- Avaya S8510 Server
- Avaya S8800 Server
- HP ProLiant DL360 G7 Server
- Dell™ PowerEdge™ R610 1U Server
- Avaya Communication Server 2x00 Server

Note the following upgrade considerations:

- Upgrade the servers on Communication Manager Release 5.2.1or Release 6.0.x to Release 6.2.1 on the existing servers.
- Upgrade the servers on Communication Manager Release 5.0 or any release earlier than 5.2.1 to Release 5.2.1 before you upgrade the servers to Release 6.2.1 unless otherwise noted.
- Upgrade the servers on a release earlier than 4.0.5 to Release 4.0.5 before you upgrade the servers to Release 6.2 unless otherwise noted.

System Platform

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:

- Easy installation of any Avaya Aura® solution template (bundled applications suite) on a single server platform
- Simpler and faster deployment of applications and solutions
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel

Avaya deploys System Platform through a *virtual appliance* model. The model includes:

- An Avaya-defined common server platform
- An Operating System (O/S) for allocating and managing server hardware resources (CPU, memory, disk storage, and network interfaces) among virtual machine instances running on the server platform
- System Platform
- An Avaya solution template containing a bundled suite of pre-integrated Avaya software applications

Communication Manager templates overview

Communication Manager as a template is a virtualized version that runs on System Platform. The Communication Manager template image has all the features that Communication Manager supports whether the image 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 Server, or Survivable Remote Server. In addition, you can use the network infrastructure of the templates 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
- Efficient licensing of applications and solutions
- Common look-and-feel Web Console (Web Graphical User Interface) for server, virtual machine, application, and overall solution management.
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel
- Coordinated backup and restore
- Coordinated software upgrades

The Communication Manager templates come in two categories: The templates in each category are as follows:

- Communication Manager for Main/Survivable Core. This category contains the following templates:
  - Simplex CM Main/Survivable Core
  - Duplex CM Main/Survivable Core
  - Embedded CM Main
- Communication Manager for Survivable Remote. This 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:

You can gain access to Communication Manager Messaging only if you configure Communication Manager as the main server. You cannot gain access to Communication Manager Messaging and Utility Services on Duplex Main/Survivable Core.

- Utility Services

You can install Simplex Main/Survivable Core and Duplex Main/Survivable Core templates on an S8510, S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server.

Note:

Avaya no longer sells the S8800 and S8510 Servers. You can only reuse the S8800 and S8510 Servers as an upgrade.

You can install the Simplex Main/Survivable Core template on an S8510 Server with a total 8-Gb memory as an upgrade only. You can install the Embedded Main template on an S8300D Server in 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

You can install the Simplex Survivable Remote on an S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. You can install Simplex Survivable Remote on an S8510 Server

with 8-Gb memory as an upgrade only. You can install Embedded Survivable Remote on S8300D Server in a G250, G350, G430, G450, or G700 Branch Gateway. You can use both the templates in the following two scenarios:

- Communication Manager Evolution Server
- Communication Manager Feature Server

Note:

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

Supported platform for survivable servers

The following table defines the platforms that you can configure as a survivable remote server or survivable core server.

Primary server	Survivable servers			
	System Platform S8300D	System Platform S8510	System Platform S8800, HP DL360 G7 or Dell R610	
			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
Simplex System Platform HP DL360 G7	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable

Primary server	Survivable servers			
Simplex System Platform Dell R610	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Not applicable
Duplex System Platform HP DL360 G7	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core
Duplex System Platform Dell R610	Survivable remote	Survivable remote or Survivable core	Survivable remote or Survivable core	Survivable core

License file for Communication Manager

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later, , and . 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 the license file. 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. The license file has the information regarding the product, major release, and license features and capacities.

For Communication Manager 6.0 and later, you must install license files on the Communication Manager main server and not on survivable servers. Survivable servers receive licensing information from the main server.

If you license a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to standby server.

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

Duplicated server licensing

If you license a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to 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. The license file that the system generates includes both host IDs. You must install that license file 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. With the ASG keys, Avaya Services can securely gain access to the customer system.

System Platform and Communication Manager share the same authentication file. The system installs a default authentication file with System Platform. However, you must replace the default file with a unique file. The Authentication File System (AFS) creates unique authentication files. AFS is an online application that you can download from 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 system automatically install the file on Communication Manager, Utility Server, and any other virtual machines on the server.

Every time you upgrade Communication Manager to a new major release, you must 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 system does not automatically synchronize the authentication file from active server to standby server.

Each survivable server must have its own unique authentication file. You must install a unique file 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 the file. 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. You cannot retain the third-party certificates as a part of the upgrade dataset, you must reinstall the third-party certificates after the upgrade. If you use third-party certificates, keep a copy or download new third-party certificates before you start the upgrade process.

Upgrade paths

The following table provides the supported upgrade paths from various releases of Communication Manager to Release 6.2.1.

Note:

You cannot upgrade some servers to Release 4.0.5 or Release 5.2.1 directly. You must upgrade to Release 4.0.5 or Release 5.2.1 on a supported server, respectively, before you complete the upgrade to Release 6.2.1.

Release	Requirement
Release 1.x.x (DEFINITY R)	Restore translations to a HP DL360 G7 or Dell R610 server on Release 6.2.1.
Release 2.x (DEFINITY SI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.1.
Release 3.x.x (DEFINITY CSI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.1.
Release 1.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.1.
Release 1.x.x (S8700)	Upgrade to Release 4.0.5 before you upgrade to Release 6.2.1 on HP DL360 G7 or Dell R610.
Release 2.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.1.
Release 2.x.x (S8500A, S8700, S8710 wDAL1)	Upgrade to Release 4.0.5 with memory upgrade before you upgrade to Release 6.2.1 on HP DL360 G7 or Dell R610. For S8710, upgrade to Release 5.2.1 before you upgrade to Release 6.2.1 on HP DL360 G7 or Dell R610. You do not require to upgrade the memory.

Release	Requirement
Release 2.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.1.
Release 3.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.1.
Release 3.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.1.
Release 4.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.1.
Release 4.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.1.
Release 5.0.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.1.
Release 5.1.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.1.
Release 5.2.1	Install a preupgrade service pack before you upgrade to Release 6.2.1.
Release 6.0.x and Release 6.2	Upgrade software-only to Release 6.2.1.

Support for SIP Enablement Services

SIP Enablement Services is not compatible with Communication Manager Release 6.x. If you upgrade Communication Manager with SIP Enablement Services Release 5.2.1 or earlier to Release 6.x, you must install Avaya Aura® Session Manager for continued support of SIP stations and adjuncts. For Session Manager options, contact an Avaya salesperson.

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 have SES on the existing system and want to use the same SIP signaling group for Session Manager:
  - To edit the **Peer Server** field, set the **Peer Detection Enabled** field to n. By default, the system sets the **Peer Detection Enabled** field to y .
  - In the **Peer Server** field, enter SM or Others.
- If the existing system has SIP integrated Modular Messaging, the upgrade process automatically prefixes a + character to the phone number.

  Important:

  You must remove the + character manually from the phone number. For instructions, see *Messaging Application Server (MAS) Administration Guide*.
- If you use Unicode phone messages on the existing system, reinstall the Unicode phone messages file after the upgrade.

Preupgrade requirements

Make sure that you:

- Order all the hardware. The hardware must be available onsite.
- Download all the software and service packs
- Have the applications you need on the computer you will use to perform the upgrade.
- Identify a server with adequate disk space to store the datasets.
- Obtain the updated translations from the STS team. You require the updated translations for DEFINITY Server upgrades only.

Hardware requirements

- HP DL360 G7 or Dell R610 Server to replace an existing standalone server that you cannot upgrade to Release 6.x
- S8300D Server to replace an existing embedded server that you cannot upgrade to Release 6.x
- Release 6.0 Migration Kit for S8510 Server or S8800 Server to reuse the existing servers
- Required Ethernet CAT5 cables
- Five blank DVDs to burn the iso images on.

Software requirements

Download the following software from the appropriate website:

- 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 Web Console Domain, as displayed on the Server Properties page of the WebLM server.
- The authentication or password file from the Authentication File System (AFS)
- Preupgrade and postupgrade service packs from the Avaya Support website at http://support.avaya.com.

Application requirements

Install the following applications on your computer:

- Internet Explorer 7.x or 8.x browser
- Firefox 2.x or 3.x browser. Only System Platform supports this browser.

  Release 6.2 supports Firefox 3.6 version and later.
- A Secure Shell application such as PuTTY.

Upgrade order

If Communication Manager is part of Avaya Aura®, perform the upgrade in the following order:

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 known as media gateways
6. Survivable core servers
7. Communication Manager, configured as feature servers and evolution servers

Upgrade process

The following list provides the general upgrade sequence for upgrade paths that start with a server running Communication Manager Release 4.0.5 and Release 5.2.1.

1. Communication Manager on any survivable remote server (formerly local survivable processors)
2. Latest firmware on all Avaya H.248 Branch Gateway
3. Latest firmware on the media modules within the H.248 Branch Gateway
4. Communication Manager on any survivable core server (formerly enterprise survivable servers)
5. Latest firmware on all TN circuit packs (if using port networks)
6. Communication Manager on the main server
7. Latest firmware on all telephones

If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

- Network Settings
- Customer Login
- DHCP DHCP Basic settings
- Branch Session Manager

Important:

The system displays the screens only for Survivable Remote and Survivable Remote Embed template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.

When you replace the server, verify the general tasks you complete on a simplex server from the following checklist:

Task	Notes	√
Make sure that the site has the server and other hardware.		
Obtain the required software and pre- and post-upgrade service packs.		
Make sure you have the server and disk space available to back up the upgrade data set. You cannot use a flashcard to restore files to System Platform.		
Make sure you have the required documentation and release notes on hand.		

Task	Notes	√
For DEFINITY Servers: • Save and freeze translations. • Send the translations to the STS team a 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.x does not support private networks (CNA and CNB). For instructions, see Introduction on page 1693.	
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.	**Important:** If you require to rollback the upgrade, you must deactivate the preupgrade patch.	
Back up the Communication Manager data set to be restored on the new server.		
Back up the Communication Manager Messaging data set that you later require to restore on the new server if messaging is enabled.		
For a standalone server, shut down the existing server and remove all power cords and cables. For 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 servers in the rack and connect the power cord and cables:	You can install a new server before completing the tasks on the existing server.	

Task	Notes	√
• HP DL360 G7 Server • Dell R610 Server • S8300D Server. Install this embedded server in a branch gateway.		
Install System Platform on the server.	On the new server, you can install System Platform before completing the tasks on the existing server.	
Get the license file from the PLDS website at https://plds.avaya.com and install it on the WebLM server that you access 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 the file 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.	
Reboot the server through System Platform Web Console or System Management Interface. **Important:** Check the status of other devices and applications that depend on Communication Manager, such as Call Management System (CMS) and Call Center. After you complete the Communication Manager upgrade, reboot the applications if required.		
Restore the Communication Manager Messaging data set through the System Management Interface.		

Task	Notes	√
Configure Communication Manager Messaging.		
Complete the postupgrade administration.		
Back up all the files.		
Register the upgraded system.		

Required documents

To complete the upgrade process, you require the following documents. See the document related to the Communication Manager product on the Avaya Support website at http://support.avaya.com.

Title	Release	Notes
Installing the Dell™ PowerEdge™ R610 Server, 03-603793	6.x.x	To install the Dell R610 Server in a rack
Installing the HP ProLiant DL360 G7 Server, 03-603799	6.x.x	To install the HP DL360 G7 Server in a rack
Quick Start for Hardware Installation: Avaya G250 Media Gateway, 03-300433	5.2.x	To install the S8300D Server in the G250 Branch Gateway
Quick Start for Hardware Installation: Avaya G350 Media Gateway, 03-300148	5.2.x	To install the S8300D Server in the G350 Branch Gateway
Quick Start for Hardware Installation: Avaya G430 Media Gateway, 03-603236	5.2.x	To install the S8300D Server in the G430 Branch Gateway
Quick Start for Hardware Installation: Avaya G450 Media Gateway, 03-602053	5.2.x	To install the S8300D Server in the G450Branch Gateway
Quick Start for Hardware Installation: Avaya G700 Media Gateway, 555-233-150	5.2.x	To install the S8300D Server in the G700 Branch Gateway
Implementing Avaya Aura® Communication Manager, 03-603558	6.x.x	To install System Platform, Communication Manager, license file, and authentication file
Installing and Upgrading the Avaya S8300 Server, 555-234-100	5.2.x	To upgrade Communication Manager to Release 5.2 on the S8300A, B, C, or D Server
Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers, 03-602885	5.2.x	To upgrade Communication Manager to Release 5.2 on

Title	Release	Notes
		the S8500 and S8700–Series Servers

Using the Upgrading to Communication Manager book

This book is organized by the Communication Manager template and then by the existing server.

To upgrade Communication Manager Release 5.2.1 on an S8500 Server to the main simplex template on an HP DL360 G7 Server, see “Upgrading S8500 Server to the HP ProLiant DL360 G7 Server” in “Upgrading to simplex main/survivable template”.

Chapter 2: Upgrading from Release 6.0.x to Release 6.2.1

Upgrading from Release 6.0.x to 6.2.1 on simplex template

Introduction

This section describes the procedure to upgrade the Communication Manager software from Release 6.0.x or 6.2 to Release 6.2.1 on the server running System Platform and the simplex main/survivable core template (CM_Simplex).

To perform this software-only upgrade, use one of the following methods:

- Onsite by connecting the laptop to the services port on the server
- Remotely by gaining the access to 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 verification tasks.
- Performing the tasks for upgrade to Release 6.2.1 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.x or 6.2 to Release 6.2.1 on:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the existing system

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Management Interface

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.

4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.

3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Before you begin

Start a SAT session.

Procedure

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

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

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

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.

     - https://<*IP_Address*>

     - https://<*FQDN*>

       Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   - This is a secure site. If you get a certificate error message, follow the instructions on 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 configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

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

     Select **Full Backup**.

     If you choose the **Full Backup** option, the resulting backup file 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.

   If the size of the backup file is large, the system creates one or more `.tar` files.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `*.tar.gz` file to the location you specify in the **Directory** field.
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 file from the list and click **Check Status**.

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

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing

system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:

   - **User Name**
   - **Password**

- **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

System Platform and Communication Manager upgrade

Perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches on page 53
- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 53

Upgrading System Platform

Before you begin

Log on to the System Platform Web Console.

About this task

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.

4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

Note:

If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

Next steps

- Install the service pack and patches for System Platform as instructed in Installing patches on page 53.
- Reconfigure the Communication Manager license server. For instructions, see Reconfiguring the Communication Manager license server on page 52.

Reconfiguring the Communication Manager license server

Before you begin

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**

- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.

   If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

   - Network Settings
   - Customer Login
   - DHCP DHCP Basic settings
   - Branch Session Manager

   Important:

   The system displays the screens only for Survivable Remote and Survivable Remote Embed template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

   Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

   Note:

   If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

   The system automatically performs the following:

   - Creates a back up of Communication Manager.

- Installs 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 53.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.
   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

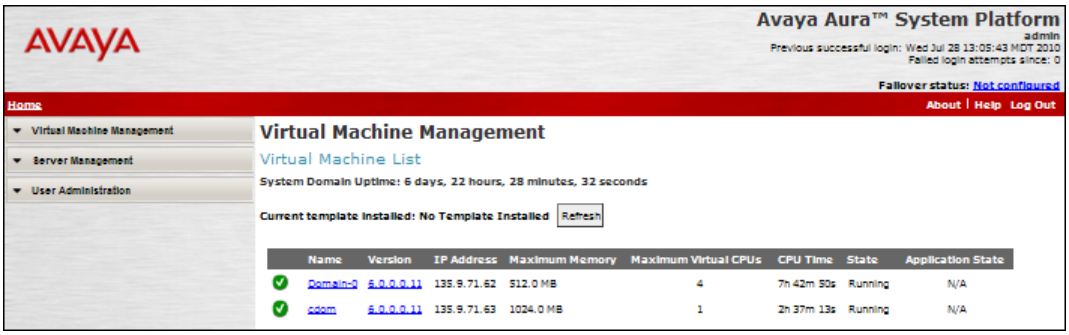
Note:

- You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.

2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading from Release 6.0.x to 6.2.1 on duplex template

Introduction

This section describes the procedure to upgrade Communication Manager software from Release 6.0.x or 6.2 to Release 6.2.1 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 the Communication Manager template.
- Performing the verification tasks.
- Performing the tasks for upgrade to Release 6.2.1 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.x or 6.2 to Release 6.2.1 on:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the active server

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Management Interface

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.

4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.

3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Before you begin

Start a SAT session.

Procedure

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

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

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

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.
   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.

     - https://<*IP_Address*>

     - https://<*FQDN*>

       Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   - This is a secure site. If you get a certificate error message, follow the instructions on 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 configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.

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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Connection preservation during an upgrade

When upgrading within the same release, for example, Release 6.0.x to Release 6.2, Communication Manager preserves 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

  For example, calls 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

  For example, links 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

Before you begin

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.

About this task

Preserve connections immediately after you perform all standard preupgrade tasks.

Procedure

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

Procedure

Unplug the portable computer from the services port.

Preupgrade tasks on the standby server

Accessing the System Management Interface

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:

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

      An alternative to the above command is **`service_port_access disable`**.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. 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.

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

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.

     - https://<*IP_Address*>

     - https://<*FQDN*>

       Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   - This is a secure site. If you get a certificate error message, follow the instructions on 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 configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Busying out the standby server

Before you begin

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Upgrade tasks on the standby server

Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

System Platform and Communication Manager upgrade

Perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches on page 53
- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 53

Upgrading System Platform

Before you begin

Log on to the System Platform Web Console.

About this task

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

Next steps

- Install the service pack and patches for System Platform as instructed in Installing patches on page 53.
- Reconfigure the Communication Manager license server. For instructions, see Reconfiguring the Communication Manager license server on page 52.

Reconfiguring the Communication Manager license server

Before you begin

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.

4. Select the Communication Manager template.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

Note:

If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

The system automatically performs the following:

- Creates a back up of Communication Manager.
- Installs 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 53.

Verifying Communication Manager operation

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. 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 the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer 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 computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.

     - https://<*IP_Address*>

     - https://<*FQDN*>

       Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   - This is a secure site. If you get a certificate error message, follow the instructions on 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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Busying out the standby server

Before you begin

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

System Platform and Communication Manager upgrade

Perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches on page 53

- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 53

Upgrading System Platform

Before you begin

Log on to the System Platform Web Console.

About this task

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

Next steps

- Install the service pack and patches for System Platform as instructed in Installing patches on page 53.
- Reconfigure the Communication Manager license server. For instructions, see Reconfiguring the Communication Manager license server on page 52.

Reconfiguring the Communication Manager license server

Before you begin

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory ***/vsp-template***:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

Note:

If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

The system automatically performs the following:

- Creates a back up of Communication Manager.
- Installs 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 53.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the active server running Release 6.2.1

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.
   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain (Cdom).

Note:

- You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.
  - https://<*IP_Address*>
  - https://<*FQDN*>

    Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).
- This is a secure site. If you get a certificate error message, follow the instructions on 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 configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the standby server running Release 6.2.1

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.

     - https://<*IP_Address*>

     - https://<*FQDN*>

       Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

   - This is a secure site. If you get a certificate error message, follow the instructions on 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 configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading from Release 6.0.x to 6.2.1 on embedded main template

Introduction

This section describes the procedure to upgrade the Communication Manager software from Release 6.0.x or 6.2 to Release 6.2.1 on the S8300D Server running System Platform and the embedded main template (CM_OnlyEmbed).

To perform this software-only upgrade, use one of the following methods:

- Onsite by connecting the laptop to the services port on the server
- Remotely by gaining the access to the server through the corporate network

The embedded main 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 verification tasks.
- Performing the tasks for upgrade to Release 6.2.1 as described in this section.

Important:

To use this section to upgrade the Communication Manager software from Release 6.0.x, or 6.2 to Release 6.2.1 on the S8300D Server running the embedded survivable remote template (CM_SurvRemoteEmbed), skip the following procedures:

- " Communication Manager Messaging backup" through "Shutting down Communication Manager Messaging"
- "Verifying the Communication Manager Messaging test data" through "Backing up Communication Manager Messaging"

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

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Verify that you have the service packs and patches for the following software: • System Platform • the required Communication Manager template	–

✔	Task	Description
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Preupgrade tasks on the existing system

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Management Interface

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.
   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Before you begin

Start a SAT session.

Procedure

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

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

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

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.

     - https://<*IP_Address*>

     - https://<*FQDN*>

       Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

- This is a secure site. If you get a certificate error message, follow the instructions on 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 configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

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

     Select **Full Backup**.

     If you choose the **Full Backup** option, the resulting backup file 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.

   If the size of the backup file is large, the system creates one or more `.tar` files.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.

5. Fill in the following fields:

   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `*.tar.gz` file to the location you specify in the **Directory** field.

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 file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Communication Manager Messaging backup

If Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

System Platform and Communication Manager upgrade

Perform the upgrade of System Platform and Communication Manager, and install the latest service packs or patches in the following order:

- System Platform
- System Platform service pack as instructed in Installing patches on page 53
- Communication Manager
- Communication Manager service pack as instructed in Installing patches on page 53

Upgrading System Platform

Before you begin

Log on to the System Platform Web Console.

About this task

Note:

After you upgrade System Platform, you must reconfigure the Communication Manager license server.

Procedure

1. In the left navigation pane, click **Server Management** > **Platform Upgrade**.
2. In the **Upgrade Platform From:** field, select a method you require to adopt.
3. Click **Search**.
4. Select the file to install for System Platform and click **Select**.
5. Click **Install**.
6. When the system prompts, click **Commit**.

   Note:

   If you fail to click **Commit**, the system rolls back to the existing release of System Platform.

Next steps

- Install the service pack and patches for System Platform as instructed in Installing patches on page 53.
- Reconfigure the Communication Manager license server. For instructions, see Reconfiguring the Communication Manager license server on page 52.

Reconfiguring the Communication Manager license server

Before you begin

Start an SSH session.

Procedure

At the prompt, type `weblmurl <ip address of license server>`.

By default, the system sets the IP address to the IP address of C-dom. If you use any other license server other C-dom, the system displays an error.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. In the left navigation pane, click **Virtual Machine Management** > **Templates**.

2. Click **Upgrade**.
3. In the **Install Template From** field, select a method to gain access to the template file.
4. Select the Communication Manager template.

   If you are upgrading Communication Manager from Release 6.0.1 or 6.2, on the survivable remote template or survivable remote embed template, the system displays the following screens. Provide the information in the appropriate fields:

   - Network Settings
   - Customer Login
   - DHCP DHCP Basic settings
   - Branch Session Manager

   Important:

   The system displays the screens only for Survivable Remote and Survivable Remote Embed template upgrades. The system does not display the screen when you upgrade the other simplex main and duplex templates.

   Click **Install** and **Finish** to complete the upgrade and install the Communication Manager patches.
5. Click **Upgrade**.
6. When the system prompts, click **Commit Installation**.

   Note:

   If you fail to click **Commit Installation**, Communication Manager remains in the current state until you click **Commit Installation**. To stay at the current Communication Manager release, click **Rollback Installation**.

   The system automatically performs the following:

   - Creates a back up of Communication Manager.
   - Installs 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 53.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

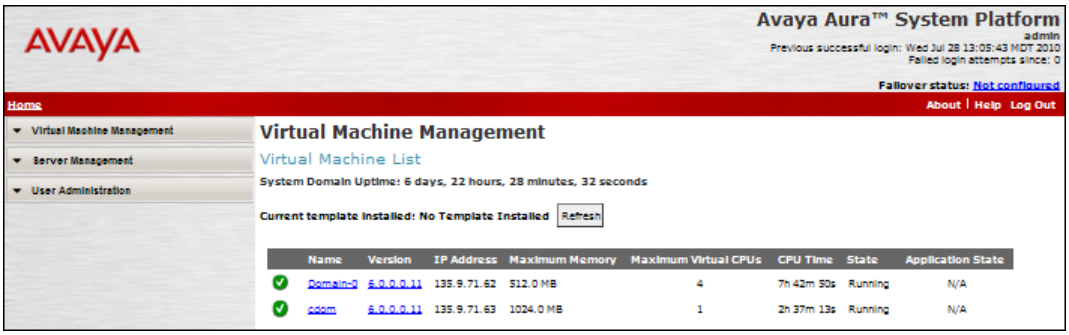
   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on 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.



Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer 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 the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade S8500A Server running Communication Manager releases 2.0 through 3.x to HP DL360 G7 Server or Dell R610 Server running Communication Manager Release 6.2.1. For the complete list of releases in this range, see the Avaya Support Web site at www.support.avaya.com.

In this upgrade procedure, you replace the S8500A Server with an HP DL360 G7 Server or a Dell 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:

- Creating a data set with specific information of the existing server that you later restore on Communication Manager Release 4.0.5.
- Upgrading Communication Manager to Release 4.0.5 on the existing server and restoring the backed up data.
- 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 6.2.1.
- Installing System Platform and Communication Manager 6.2 on a new 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 6.2.1.

Use this section to upgrade Communication Manager from releases 2.0 through 3.x to Release 6.2.1:

- 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

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:

a. Right-click and select **Paste**.

   The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.

    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

Before you begin

To use Telnet, enable the Telnet service for Communication Manager.

About this task

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

Procedure

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, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, 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

Procedure

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)

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

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

If the backup file size is large, there may be more than one `.tar` file.

5. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
6. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**
7. Click **Start Backup**.
8. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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)

About this task

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

Procedure

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 service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new 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

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

   You can select four files at a time.
6. 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

Before you begin

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

About this task

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.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.
   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`, where *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name. .
   The 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. To view the status of the processes, enter `statapp -c`.
    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

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

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 a flashcard

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **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, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter 3.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up files to localhost

Before you begin

Enable the FTP service.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, 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. In the **Backup Method** section, 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services laptop computer using FTP

About this task

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.
   Note the name of the directory, you need the name 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 portable computer from the server

Procedure

Disconnect the services portable 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 a new server that supports Release 4.0.5

New server that supports Release 4.0.5

Complete the upgrade procedures described in the following sections on a new server that supports Communication Manager Release 4.0.5. For example, S8500 B or S8500C. At this point, you turn on the new server but you do not connect to the network.

Installing Communication Manager

Use this procedure to install Communication Manager Release 4.0.5 or Release 5.2.

Before you begin

- Install the new server, which supports Communication Manager release you want to install, in the rack.
- Insert the CD-ROM for Communication Manager Release 5.2.1 or Release 4.0.5 into the drive of the server.
- Turn on the server.

Procedure

1. On the portable computer, 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

Procedure

1. On the computer, 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 option 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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

Before you begin

Log on to System Management Interface.

Procedure

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

Copying files to the server

Before you begin

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

About this task

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`

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing service pack

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Creating a super-user login

About this task

Note:

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

Procedure

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

About this task

⚠ 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 153.

Procedure

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. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `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

Before you begin

- Log on to System Management Interface.
- 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.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. 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**.
4. Click **View**.
5. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
6. Select both **Force** options.
7. Click **Restore**.
8. 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

About this task

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.

Procedure

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 computer to the server

Before you begin

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

About this task

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

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

Procedure

1. Disconnect the laptop from the Ethernet port labeled **2**.

2. Connect the laptop to the Ethernet port labeled **4**.

Accessing System Management Interface

About this task

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

Procedure

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

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.

3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up files to localhost

Before you begin

Enable the FTP service.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. In the **Data Sets** section, 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. In the **Backup Method** section, 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 file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services portable computer using FTP

About this task

Log on to the services portable computer.

Procedure

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

   Note the name of the directory, you need the name 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Upgrade tasks on the HP DL360 G7 or Dell R610 (Release 6.2) Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Turning on the server

Before you begin

Do not connect the server to the network.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

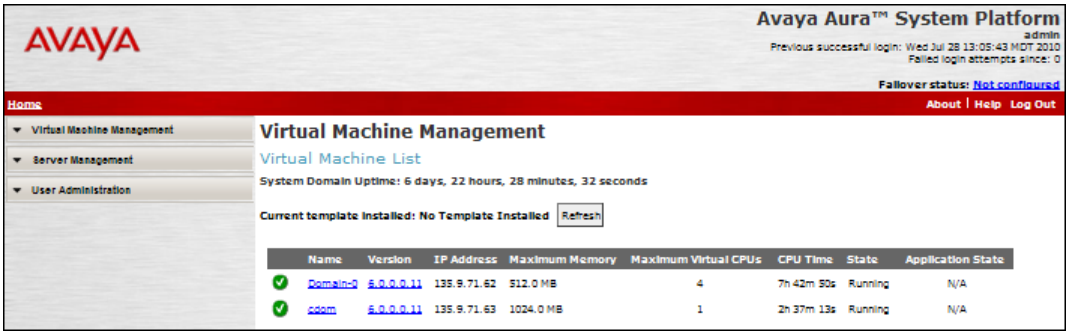
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying the upgrade dataset from the laptop to the server

Procedure

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

   Note:

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

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the S8500A Server

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Postupgrade tasks on the HP DL360 G7 or Dell R610 (Release 6.2) Server

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:

- To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
- To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500-Series Server to the HP DL360 G7 or Dell R610 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 6.2.1 on HP DL360 G7 Server or Dell R610 Server.

In this upgrade procedure, you replace the S8500B or S8500C Server by an HP DL360 G7 Server or Dell 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:

- 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 6.2.1.

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 6.2.1.

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 the 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 6.2.1.
3. Perform the upgrade to Release 6.2.1 as described in this section.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.2.1:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on 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

You need the following additional documentation:

✔	Task	Description
	Obtain one of the following as appropriate: • *Installing the HP DL360 G7 Server* (03-603799) • *Installing the Dell R610 Server* (03-603793)	Provides instructions for installing the 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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware

2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8500 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:

a. Right-click and select **Paste**.

   The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

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

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations (main only)

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

     iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

     iv. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

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

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.

7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.

- For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Disconnect the laptop from the Services port.
2. Label and disconnect the power cords 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

Procedure

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 target server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

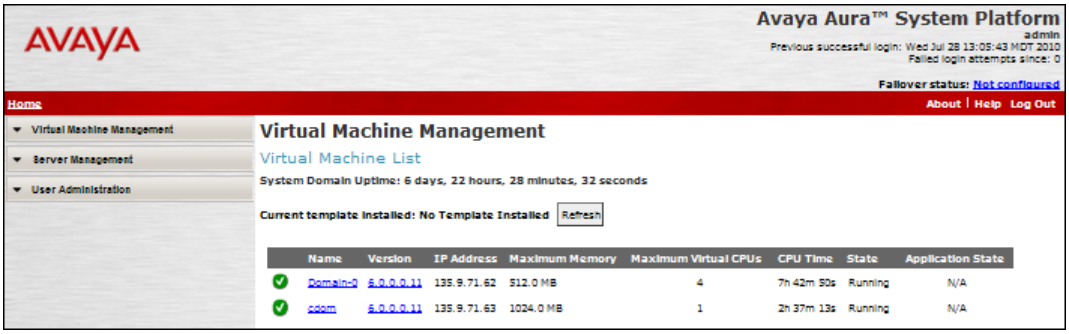
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.

4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.
   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:

- To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
- To use 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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer 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 6.2.1 running System Platform and the simplex main/survivable core template (CM_Simplex) for the 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 6.2.1.

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 6.2.1.

You can reuse the existing server. However, if the current hard disks have 146 GB memory, perform the following additional tasks:

- Increase the memory.
- Remove the Server Availability Management Processor (SAMP) board.
- (Optional) Add a third hard disk drive but only if the current hard disks are of the SAS type with 146-GB memory.
- (Optional) Reconfigure to RAID 5 but 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 6.2.1 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

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware

3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:

   a. Right-click and select **Paste**.

The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.
c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

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

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations (main only)

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

     iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

     iv. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Verifying the hardware on the server

Before you begin

Log on to System Management Interface.

About this task

Perform the following steps to determine:

- The need to install an additional hard disk drive on the server to support Communication Manager
- RAID configuration on the server

Procedure

1. On the **Administration** menu, click **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

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:

- **User Name**
- **Password**
- **Host Name**
- **Directory**

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

4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the front bezel from the server

About this task

Caution:

Wear an antistatic wrist ground strap before you handle any 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.

Procedure

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

Procedure

1. Label and disconnect the power cords 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 behind the server.

5. Disconnect the LAN cable, if used, from the Ethernet port on the SAMP behind the server.

Removing the server from the rack

Before you begin

⚠ Caution:

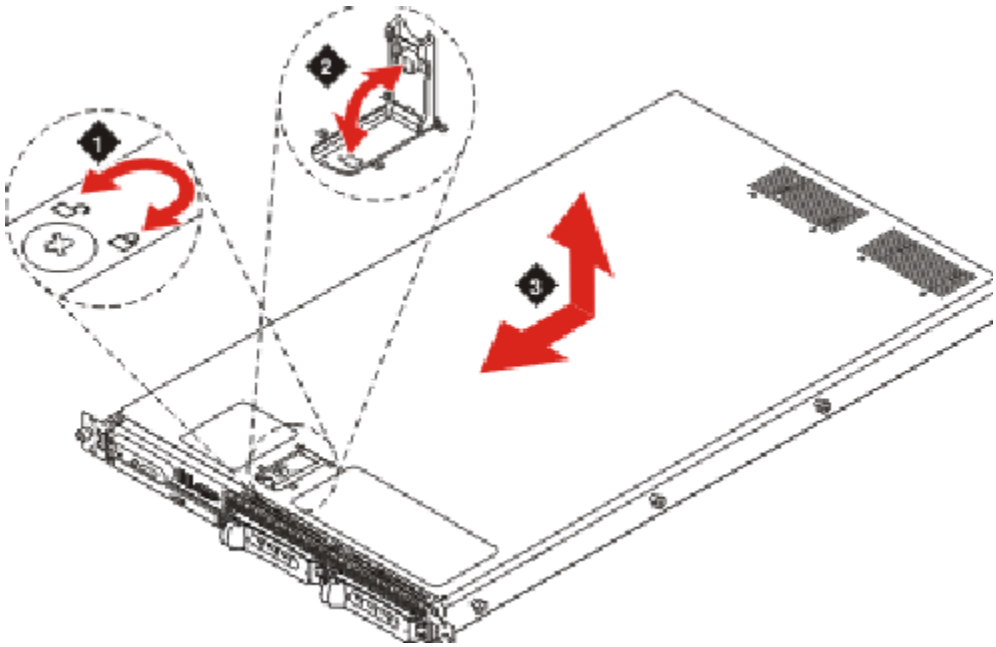
Detach the power cords from the power source to disconnect the server completely.

Procedure

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

About this task



Procedure

1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver. See Figure 1.
2. Lift the latch up to unlock. See Figure 2.
3. Slide the cover back and lift straight up to remove. See Figure 3.

Adding the memory modules

About this task

⚠ Caution:

Ensure that you wear electrostatic wrist ground strap on your bare wrist.

Procedure

1. Remove the protective cover over the memory modules.
2. Insert the new memory modules.

Removing the SAMP

Before you begin

You must remove all power from the server and the SAMP card. The SAMP has a separate power source from the server.

⚠ Electrostatic alert:

Wear a wrist strap connected to an approved ground.

About this task

The SAMP card resides in a PCI expansion card riser at the rear of the server.

Procedure

1. Lift the release latches on the PCI expansion card riser.
2. Disconnect the cable assembly from the SAMP and set the cable aside. You do not reuse the cable but 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 disk drive

Before you begin

- Verify if you need a third hard disk drive. For instructions, see Verifying the hardware on the server on page 223.
- Remove the front bezel and the cover of the server.

Procedure

1. Pinch together the two tabs of the drive carrier release handle.
2. Open the carrier release handle.
3. Insert the hard disk drive into the slot and push the hard disk drive inside until the drive is seated.
4. Close the hard drive carrier handle to lock the hard disk drive in place.

Replacing the S8510 Server cover

Procedure

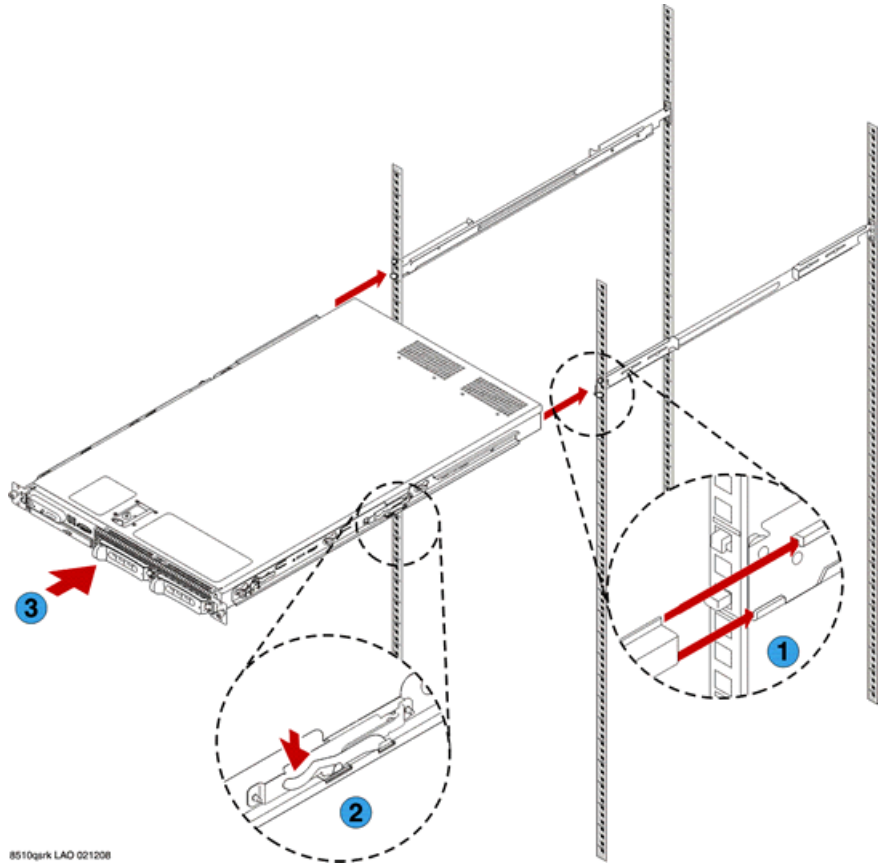
1. Place the cover on top of the server, aligning the cover with the J hooks on the sides.
2. Slide the cover forward.
3. Push the latch down to lock.
4. Rotate the latch release lock clockwise to secure the cover.

Installing the server in the rack

Before you begin

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.

Procedure



Next steps

If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Replacing the front bezel

Procedure

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

Before you begin

CD comcoded 700500415

About this task

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.

Procedure

1. Insert the CD comcoded 700500415 into the hard 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-ROM 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-ROM from the drive and press `Enter` to reboot the server.

   Alternatively, wait for 2 minutes, the system reboots automatically.

Upgrade tasks

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

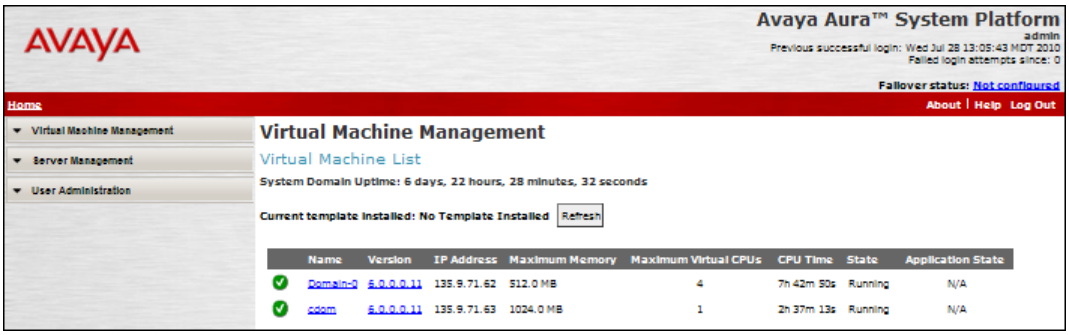
Note:

- You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Installing service pack

Before you begin

- Copy the latest service packs from the Avaya Support Site to the services portable computer.
- Log on to System Platform Web Console.

About this task

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.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets.
See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:

- **Server Hardware**: okay
- **Processes**: okay

4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.

2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer 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 6.2.1. In this procedure, you reuse the S8800 Server and install System Platform and the simplex main/survivable core template, CM_Simplex, 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 6.2.1.

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 6.2.1.

Perform the following additional tasks to reuse the existing server:

- Increase the memory.
- Add a third hard disk 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 *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	For the list of required equipment, see *Avaya Migration Kit.*

✔	Task	Description
	• Services laptop and crossover cable • Electrostatic wrist ground strap and mat	
	Obtain the CD-ROM to update the uEFI firmware using one of the following ways: • Order the *uEFI firmware* CD-ROM • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD-ROM.	
	Obtain the *RIAD 5 firmware* CD-ROM	
	Obtain the CD-ROM to update the uEFI settings using one of the following ways: • Order the *uEFI settings* CD-ROM • Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD-ROM.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.

3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations (main only)

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

     iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

     iv. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address

- **Directory**

When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Verifying the hardware on the server

Before you begin

Log on to System Management Interface.

About this task

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.
   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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

Before you begin

Before you disconnect the server from the power source, note which LEDs are lit, including the LEDs that are lit on the operation information panel and 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 do not light up when the power source is removed.

About this task

Remove the server cover to access the server's internal components.

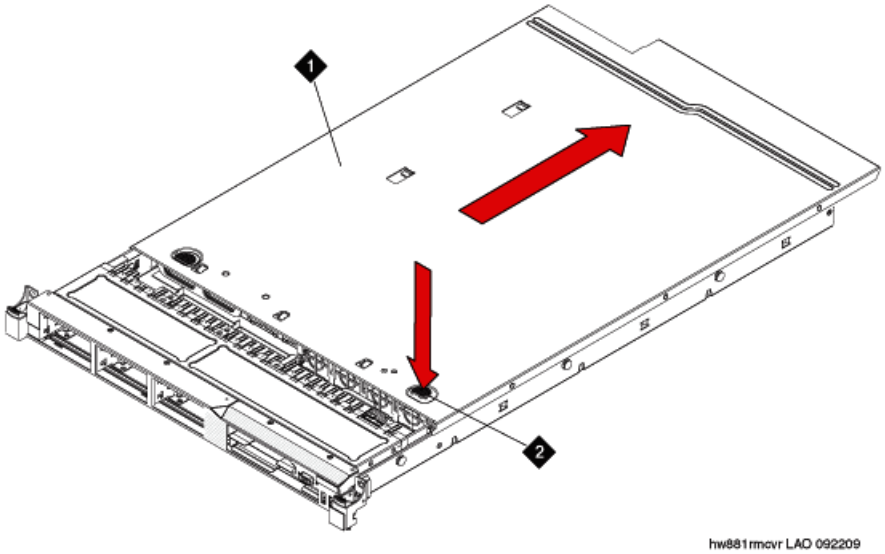
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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

About this task

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

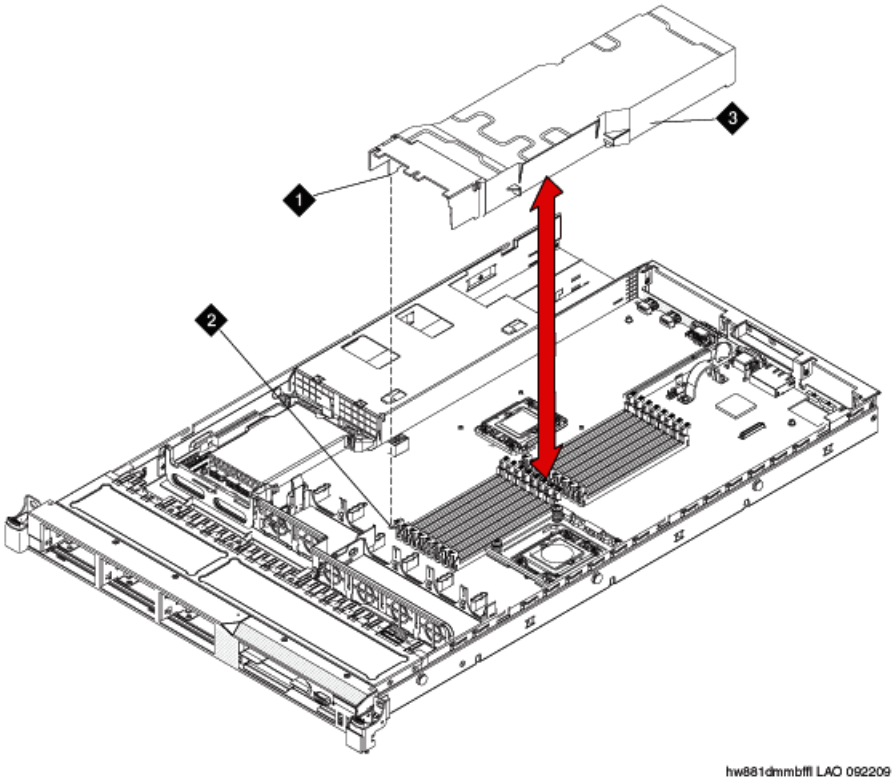
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM 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

Before you begin

Remove the DIMM air baffle.

About this task

Important:

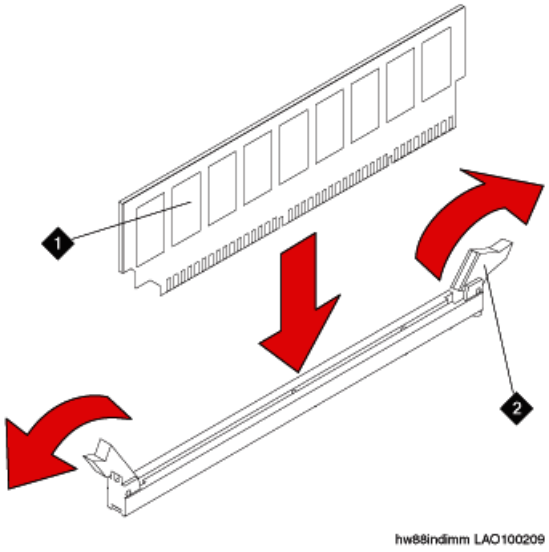
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

About this task

You must install the DIMM air baffle after you install a memory module.

Caution:

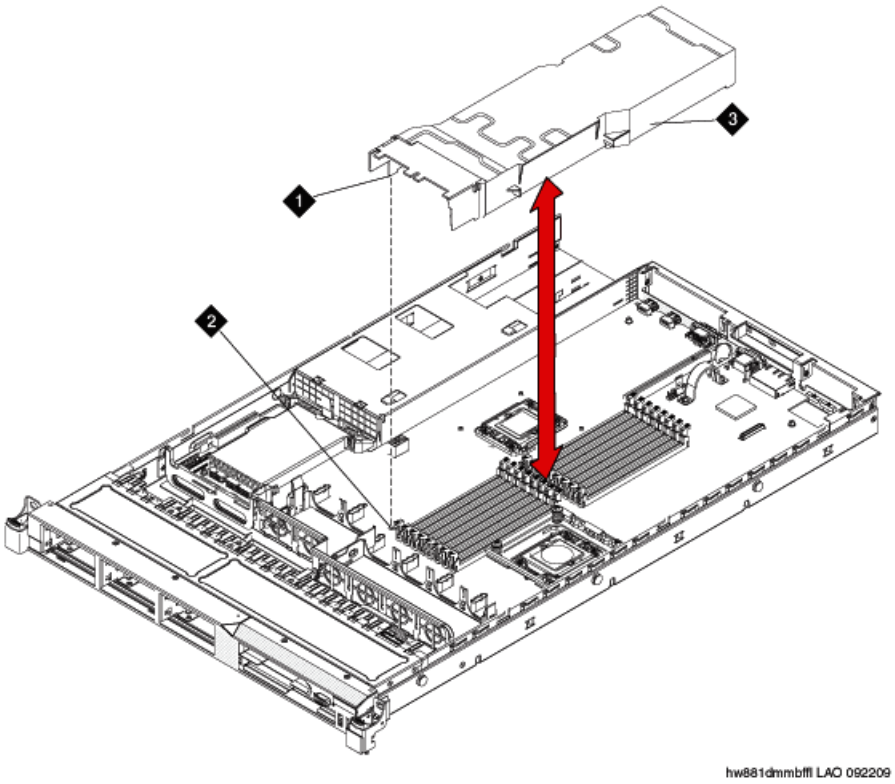
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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 the 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

Before you begin

If replacing an existing hard drive, remove the hard drive that you want to replace.

About this task

Important:

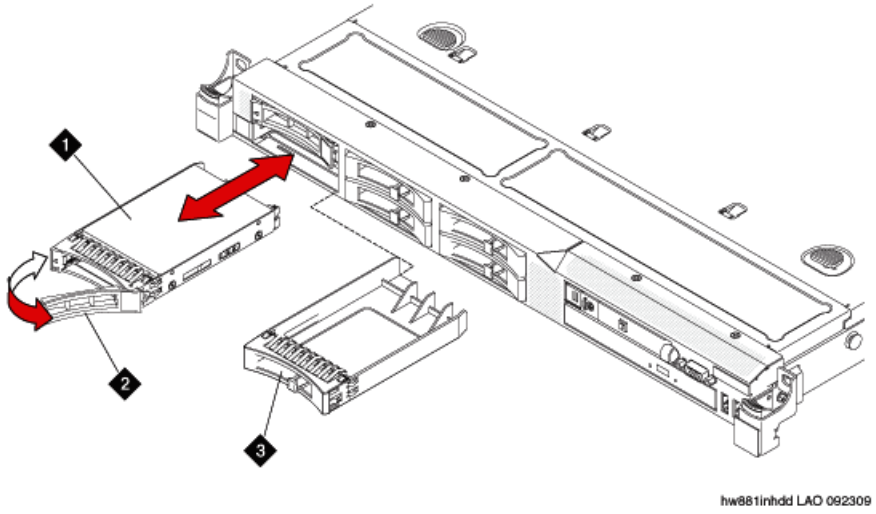
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

Before you begin

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Before you begin

- 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.

About this task

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.

Procedure

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

Before you begin

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

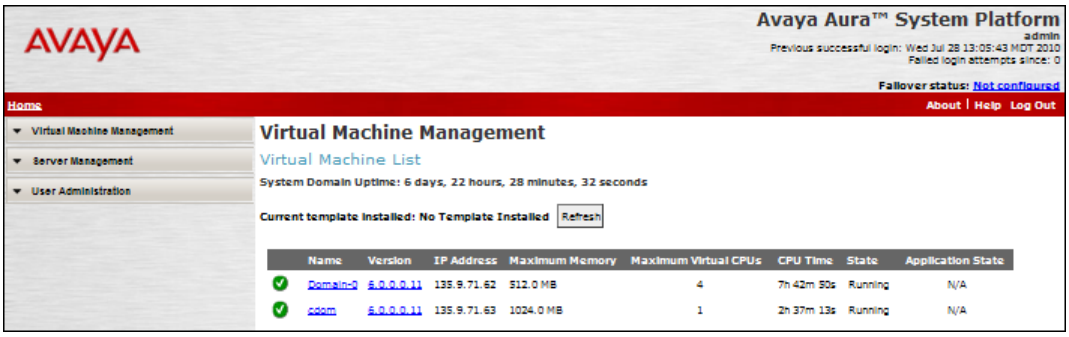
1. Open a compatible Internet browser on your computer.
   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on 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.



Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory */vsp-template*:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.

4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   Important:

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.

6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.

4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system

Before you begin

Start a SAT session.

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Busying out previously busied out equipment

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.

2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the S8800 Server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 on S8800 Server to Release 6.2.1 on HP DL360 G7 Server or Dell R610 Server.

In this upgrade procedure, you:

- Replace one of the following:
  - S8800 Server with an HP DL360 G7 Server or Dell R610 Server
  - HP DL360 G7 Server with a Dell R610 Server
- Install System Platform and the simplex main template (CM_Simplex) on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with a new G450 or G430 Branch Gateway.

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 6.2.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration.

You require a new license for Communication Manager.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.2.1 on:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the following software: • System Platform • the required Communication Manager template	_
	Obtain one of the following servers, as appropriate: • HP DL360 G7 • Dell R610	_
	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* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

You need the following additional documentation:

✔	Task	Description
	Obtain one of the following as appropriate: • *Installing the HP DL360 G7 Server* (03-603799) • *Installing the Dell R610 Server* (03-603793)	Provides instructions for installing the 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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8800 Server

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.

2. In the browser, choose one of the following options depending on server configuration:

   • LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

   • LAN access by host name

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

   • Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

- To log 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`.
- To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, 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)**

     iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

     iv. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You

must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

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

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a

test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    ⚠ Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutdown tasks on S8800 Server

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

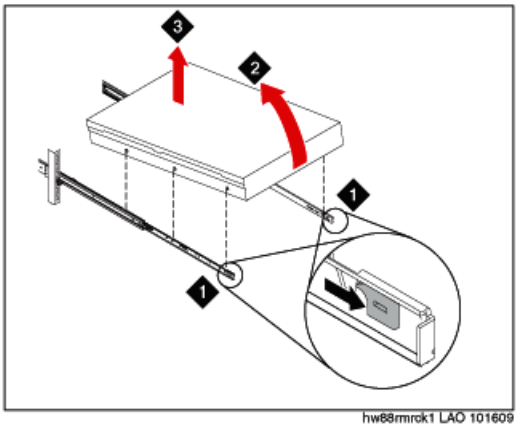
Procedure

1. Label and disconnect the power cords 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 from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

Upgrade tasks on the target server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

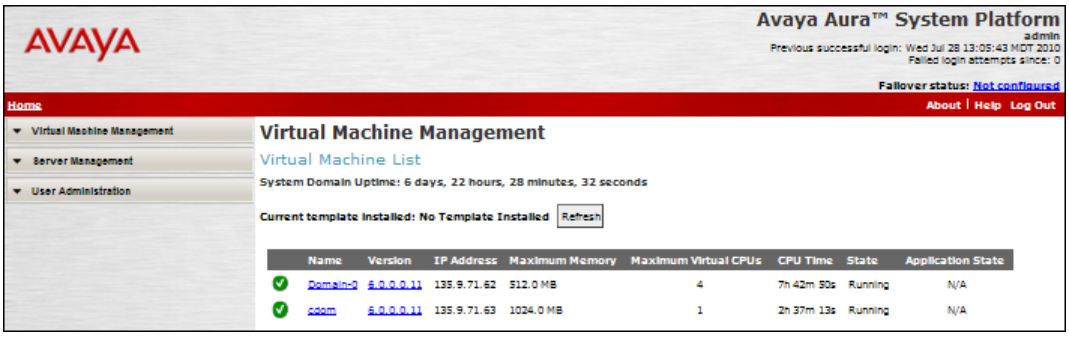
   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.

4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   Important:

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.

6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.

4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.

5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 to Release 6.2.1 on HP DL360 G7 Server.

In this upgrade procedure, you:

- Reuse the HP DL360 G7 Server.
- Install System Platform and the simplex main/survivable core template (CM_Simplex) on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with a new G450 or G430 Branch Gateway.

The simplex main/survivable core template supports:

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

You require a new license for Communication Manager.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.2.1 on:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.

✔	Task	Description
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server

5. Communication Manager on a main server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.

2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Verifying the hardware on the server

Before you begin

Log on to System Management Interface.

About this task

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Server Configuration** > **Display Configuration**.
   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:

- **User Name**
- **Password**
- **Host Name**
- **Directory**

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

4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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.

Upgrade tasks

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

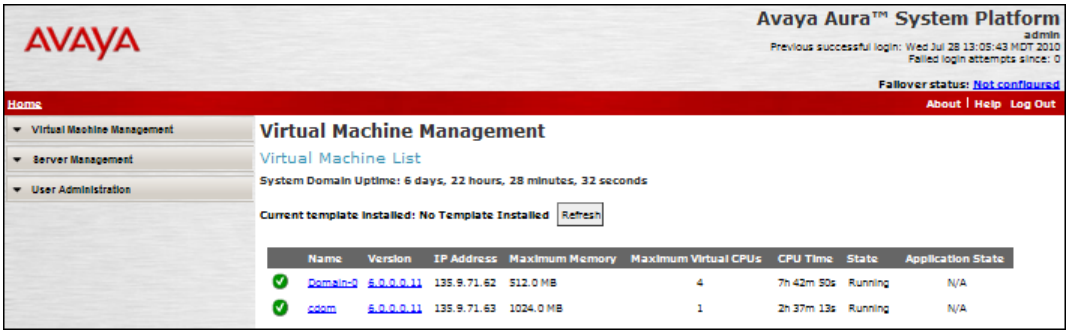
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack

- Solution template service packs
- Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets.
See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

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

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Testing the system

Before you begin

Start a SAT session.

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Busying out previously busied out equipment

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading DEFINITY SI or R Server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the following servers to Communication Manager Release 6.2 on an HP DL360 G7 Server or Dell 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 HP DL360 G7 Server or Dell 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 6.2 on the new server.
- Installing translation file on Communication Manager Release 6.2.
- Administering IPSIs on Communication Manager Release 6.2.
- 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 6.2.

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: - HP DL360 G7 - Dell R610 • 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.

✔	Task	Description
	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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

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

Before you begin

A cross-over cable to connect your services laptop directly to the processor.

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Procedure

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

Procedure

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, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

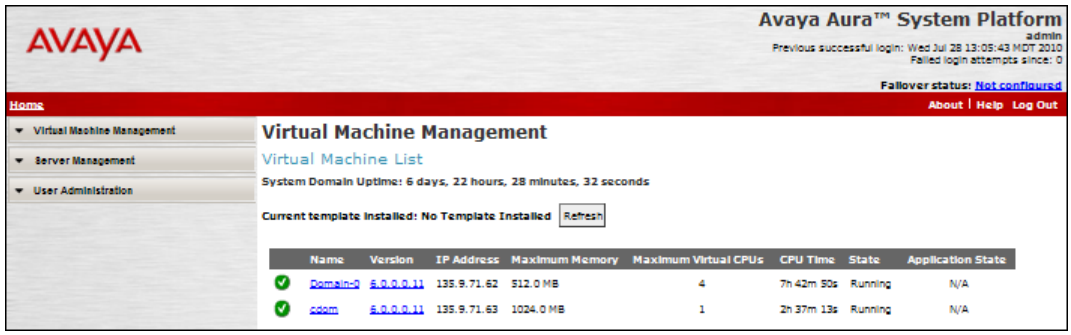
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

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

Note:

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

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

Before you begin

Log on to System Management Interface.

About this task

You restore the translations only on the main server. When a 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server 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 status of restore process.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.

2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the 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 pack

Before you begin

Start a SAT session.

About this task

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

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 in the **Circuit Packs Available for Synchronization** section.

5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for 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 all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display PASS in the **Results** field. If the **Results** field does not display PASS, troubleshoot the synchronization error.

Completion tasks on the cabinet

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

About this task

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

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 HP DL360 G7 Server or a Dell R610 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 load balance across the IPSIs throughout the port networks.

Removing the processor port network control cabinet

About this task

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

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 if you want 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

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431

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

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.

- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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 the HP DL360 G7 or Dell R610 Server

Introduction

Use this procedure to upgrade S8500A Server running Communication Manager releases 2.0 through 3.x to an HP DL360 G7 Server or a Dell R610 Server running Communication Manager Release 6.2.1. For the complete list of releases in this range, see the Avaya Support Web site at www.support.avaya.com.

In this upgrade procedure you replace the S8500A Server configured as survivable remote processor with an HP DL360 G7 Server or Dell R610 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 new server.
- Installing System Platform and Communication Manager survivable remote template on the new 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 6.2.1 configured as survivable remote server.

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.
    c. Enter `almsnmpconf` and record the output.

Recording the scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Record the backup scheduled for the existing server. You must submit the scheduled backups after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.

3. On the Schedule Backup page, note the details of any backup schedules.

   You submit these scheduled backups after the upgrade on the new server running Communication Manager Release 6.0.x.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     i. Click **Specify Data Sets**.
     ii. Select the check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.
   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
6. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**
7. Click **Start Backup**.
8. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Upgrade tasks on the Release 6.2.1 Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

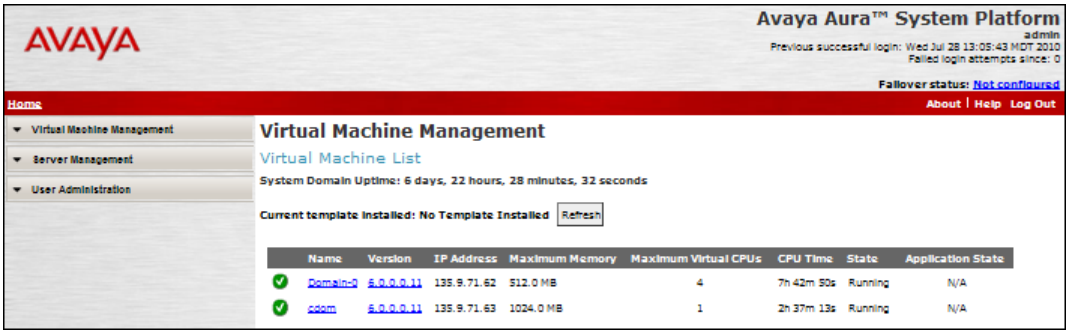
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Configuring the alarming information

Before you begin

Log on to System Management Interface.

About this task

Configure the information provided in the worksheet available in Appendix A on page 1661.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter a `lmsnmpconf` 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

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Submitting the scheduled backups

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500-Series Server to the HP DL360 G7 or Dell R610 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 6.2.1.

In this upgrade procedure, you replace the S8500B or S8500C Server by an HP DL360 G7 Server or Dell R610 Server running System Platform and the simplex survivable remote template (CM_SurvRemote).

The simplex survivable remote template supports 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 6.2.1.

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 6.2.1.

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 6.2.1.
3. Perform the upgrade to Release 6.2.1 as described in this section.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.

✔	Task	Description
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on 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

You need the following additional documentation:

✔	Task	Description
	Obtain one of the following as appropriate: • *Installing the HP DL360 G7 Server* (03-603799) • *Installing the Dell R610 Server* (03-603793)	Provides instructions for installing the 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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8500-Series Server

Accessing the System Management Interface

About this task

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

Procedure

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

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

- To log 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`.
- To log in from a portable computer 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 the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.

4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**

- **Host Name**
- **Directory**

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

4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Procedure

1. Disconnect the laptop from the Services port.
2. Label and disconnect the power cords 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

Procedure

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 HP DL360 G7 or Dell R610 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

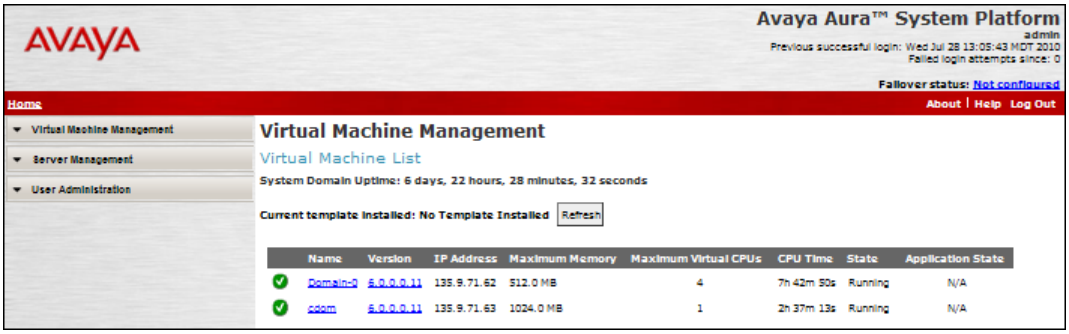
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer 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 6.2.1 running System Platform and the simplex survivable remote template for existing Communication Manager on S8510 Server.

The simplex survivable remote template supports 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 6.2.1.

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 6.2.1.

You can reuse the existing server. However, if the current hard disks have 146 GB memory, perform the following additional tasks:

- Increase the memory.
- Remove the Server Availability Management Processor (SAMP) board.
- (Optional) Add a third hard disk drive but only if the current hard disks are of the SAS type with 146-GB memory.
- (Optional) Reconfigure to RAID 5 but 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

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8510 Server

Accessing the System Management Interface

About this task

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

Procedure

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

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

- To log 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`.
- To log in from a portable computer 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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:

   • **User Name**

   • **Password**

   • **Host Name** which is the host IP address

   • **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the front bezel from the server

About this task

Caution:

Wear an antistatic wrist ground strap before you handle any 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.

Procedure

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

Procedure

1. Label and disconnect the power cords 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 behind the server.
5. Disconnect the LAN cable, if used, from the Ethernet port on the SAMP behind the server.

Removing the server from the rack

Before you begin

⚠ Caution:

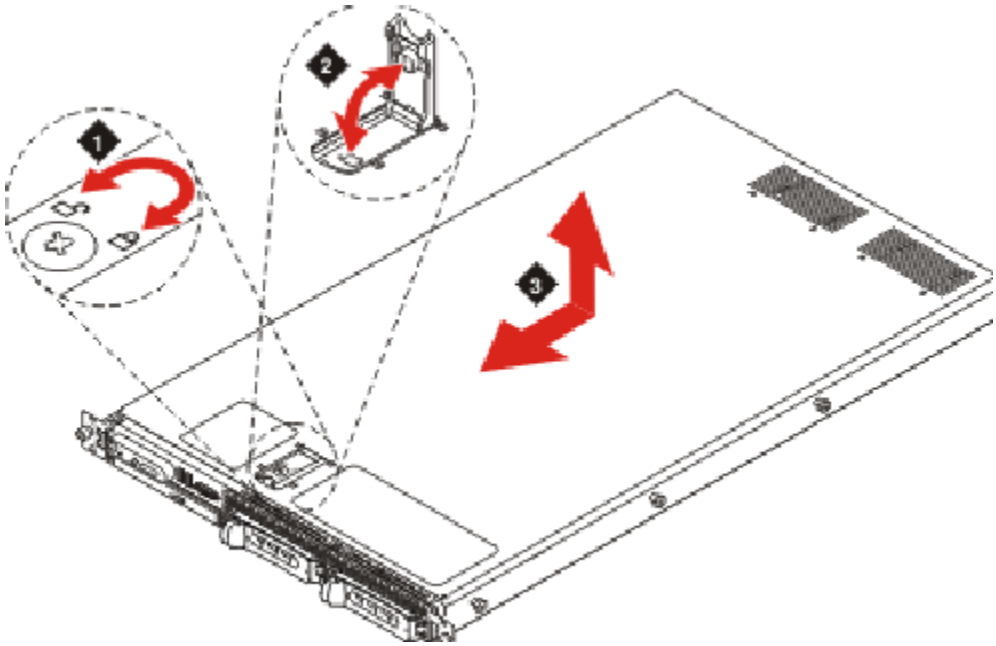
Detach the power cords from the power source to disconnect the server completely.

Procedure

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

About this task



Procedure

1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver. See Figure 1.
2. Lift the latch up to unlock. See Figure 2.

3. Slide the cover back and lift straight up to remove. See Figure 3.

Adding the memory modules

About this task

⚠ Caution:

Ensure that you wear electrostatic wrist ground strap on your bare wrist.

Procedure

1. Remove the protective cover over the memory modules.
2. Insert the new memory modules.

Removing the SAMP

Before you begin

You must remove all power from the server and the SAMP card. The SAMP has a separate power source from the server.

⚠ Electrostatic alert:

Wear a wrist strap connected to an approved ground.

About this task

The SAMP card resides in a PCI expansion card riser at the rear of the server.

Procedure

1. Lift the release latches on the PCI expansion card riser.
2. Disconnect the cable assembly from the SAMP and set the cable aside. You do not reuse the cable but 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 disk drive

Before you begin

- Verify if you need a third hard disk drive. For instructions, see Verifying the hardware on the server on page 223.
- Remove the front bezel and the cover of the server.

Procedure

1. Pinch together the two tabs of the drive carrier release handle.
2. Open the carrier release handle.
3. Insert the hard disk drive into the slot and push the hard disk drive inside until the drive is seated.
4. Close the hard drive carrier handle to lock the hard disk drive in place.

Replacing the S8510 Server cover

Procedure

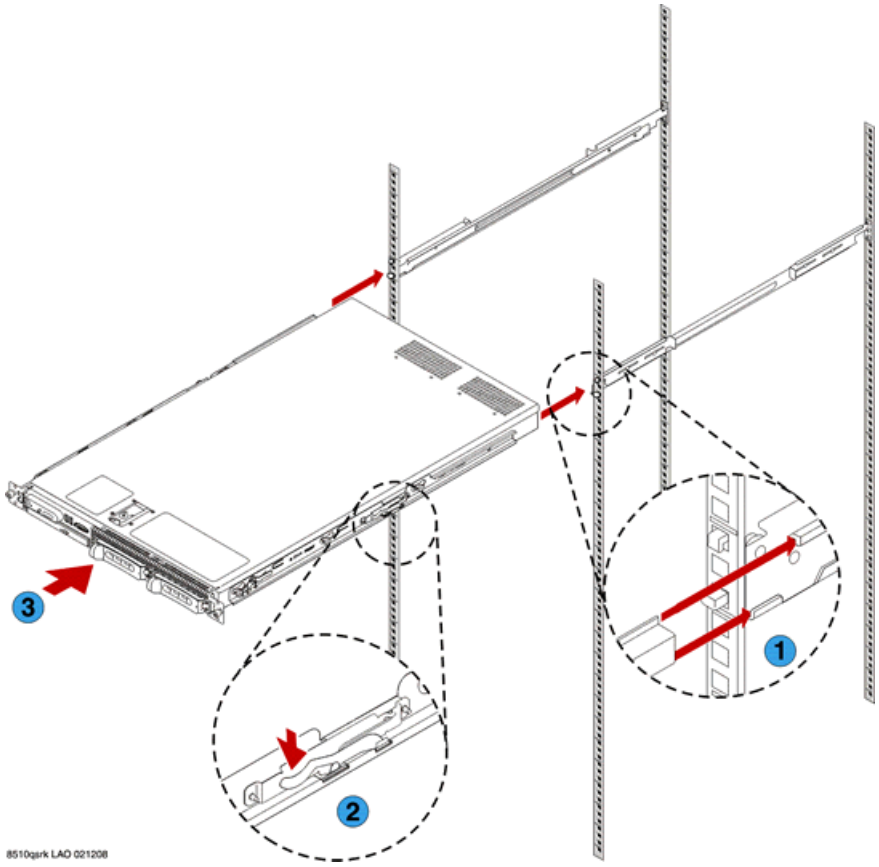
1. Place the cover on top of the server, aligning the cover with the J hooks on the sides.
2. Slide the cover forward.
3. Push the latch down to lock.
4. Rotate the latch release lock clockwise to secure the cover.

Installing the server in the rack

Before you begin

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.

Procedure



Next steps

If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Replacing the front bezel

Procedure

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

Before you begin

CD comcoded 700500415

About this task

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.

Procedure

1. Insert the CD comcoded 700500415 into the hard 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-ROM 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-ROM from the drive and press `Enter` to reboot the server.

   Alternatively, wait for 2 minutes, the system reboots automatically.

Upgrade tasks

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

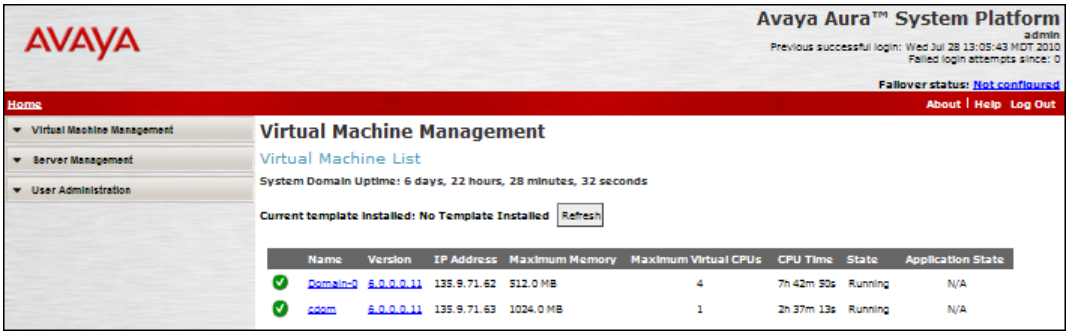
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:

a. Log on to System Management Interface.
b. On the **Administration** menu, click **Server (Maintenance)**.
c. Click **Server** > **Process Status**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer 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 6.2.1 on the existing S8800 Server. using System Platform and the simplex survivable remote template on S8800 Server.

In this procedure, you reuse the existing S8800 Server and install System Platform and the simplex survivable remote template, CM_SurvRemote, on the server.

The simplex survivable remote template supports 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 6.2.1.

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 6.2.1.

Perform the following additional tasks to reuse the existing server:

- Increase the memory.
- Add a third hard disk 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 *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	

✔	Task	Description
	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-ROM to update the uEFI firmware using one of the following ways: • Order the *uEFI firmware* CD-ROM • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD-ROM.	
	Obtain the *RIAD 5 firmware* CD-ROM	
	Obtain the CD-ROM to update the uEFI settings using one of the following ways: • Order the *uEFI settings* CD-ROM • Download the `S8800uEFITool.iso` file from Avaya Support Site and create a CD-ROM.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.

2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Verifying the hardware on the server

Before you begin

Log on to System Management Interface.

About this task

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.

   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

   You can select four files at a time.

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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

Before you begin

Before you disconnect the server from the power source, note which LEDs are lit, including the LEDs that are lit on the operation information panel and 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 do not light up when the power source is removed.

About this task

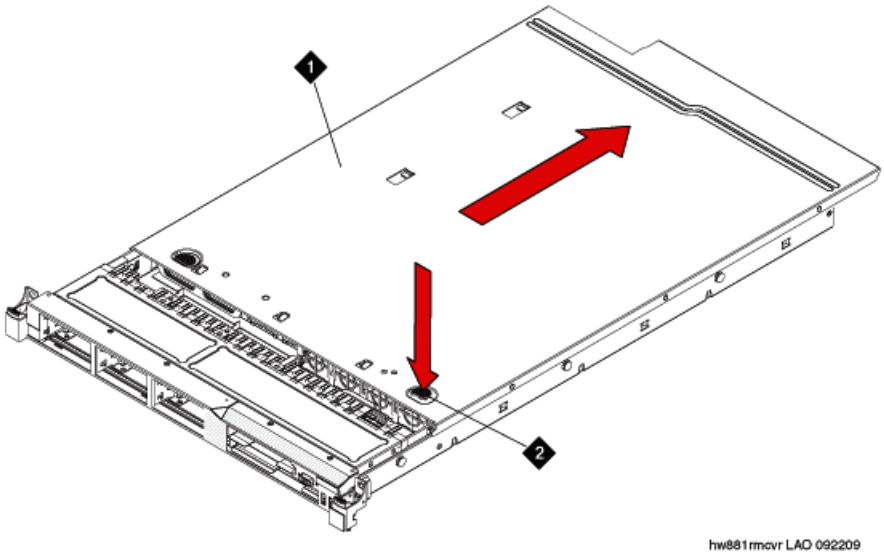
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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

About this task

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

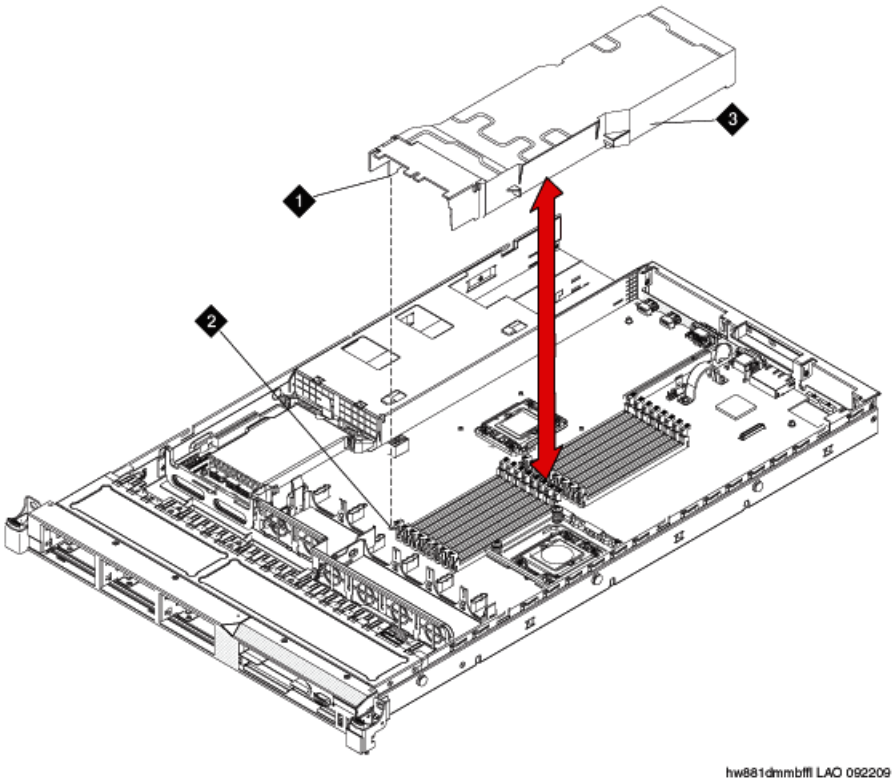
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM 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

Before you begin

Remove the DIMM air baffle.

About this task

Important:

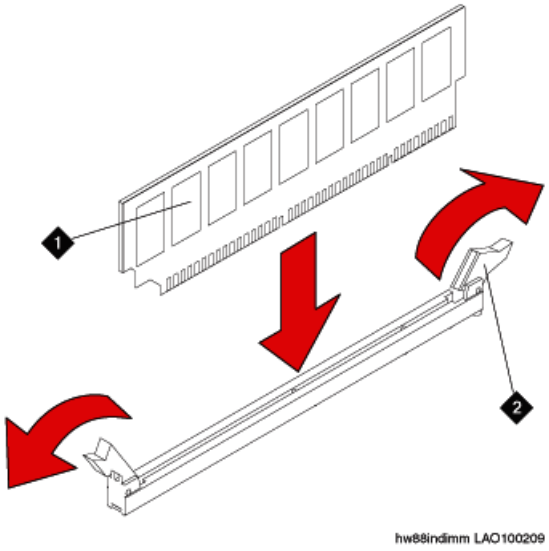
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

About this task

You must install the DIMM air baffle after you install a memory module.

Caution:

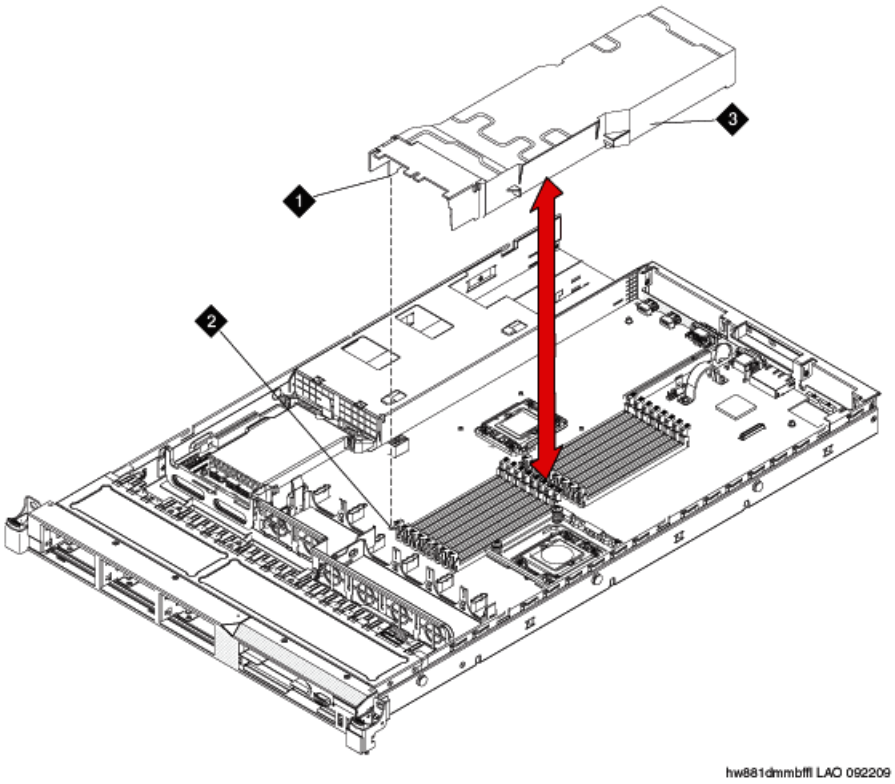
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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 the 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

Before you begin

If replacing an existing hard drive, remove the hard drive that you want to replace.

About this task

Important:

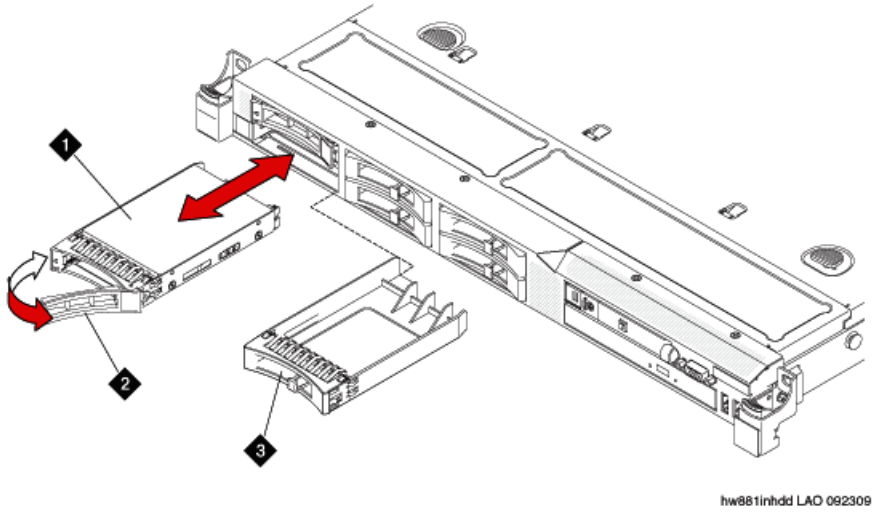
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

Before you begin

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Before you begin

- 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.

About this task

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.

Procedure

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

Before you begin

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

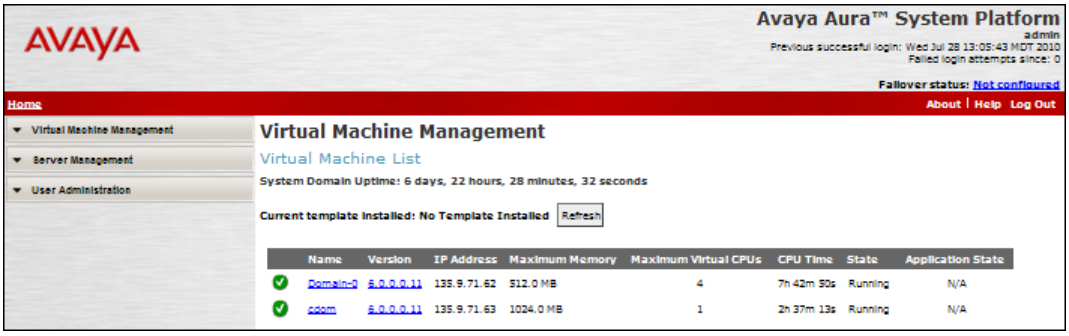
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:

a. Log on to System Management Interface.
b. On the **Administration** menu, click **Server (Maintenance)**.
c. Click **Server** > **Process Status**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the S8800 Server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 on S8800 Server to Release 6.2.1 on HP DL360 G7 Server or Dell R610 Server.

The simplex survivable remote template supports Utility Services.

In this upgrade procedure, you:

- Replace one of the following:
  - S8800 Server with an HP DL360 G7 Server or Dell R610 Server
  - HP DL360 G7 Server with a Dell R610 Server
- Install System Platform and the simplex survivable remote template (CM_SurvRemote) on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with a new G450 or G430 Branch Gateway.

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 6.2.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration.

You require a new license for Communication Manager.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on 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

You need the following additional documentation:

✔	Task	Description
	Obtain one of the following as appropriate: • *Installing the HP DL360 G7 Server* (03-603799) • *Installing the Dell R610 Server* (03-603793)	Provides instructions for installing the 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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8800 Server

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.

2. In the browser, choose one of the following options depending on server configuration:

   • LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

   • LAN access by host name

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

   • Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

- To log 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`.
- To log in from a portable computer 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 the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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`.

Shutdown tasks on S8800 Server

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

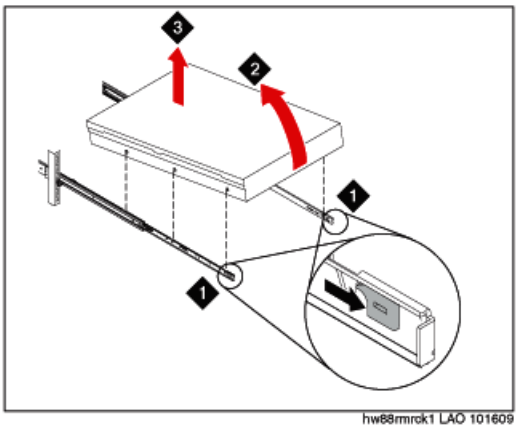
Procedure

1. Label and disconnect the power cords 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 from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

Upgrade tasks on the HP DL360 G7 or Dell R610 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

c. In the command line, type **ip_forwarding disable** and press **Enter**.

An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

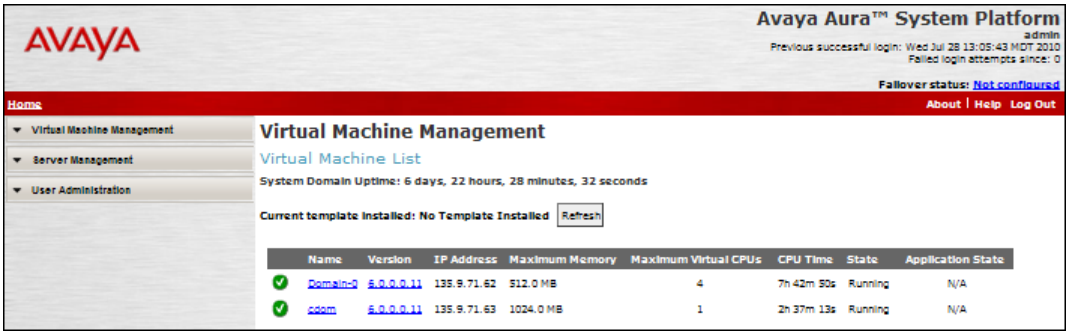
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:

a. Log on to System Management Interface.
b. On the **Administration** menu, click **Server (Maintenance)**.
c. Click **Server** > **Process Status**.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 to Release 6.2.1 on HP DL360 G7 Server.

In this upgrade procedure, you:

- Reuse the HP DL360 G7 Server.
- Install System Platform and the survivable remote template (CM_SurvRemote) on the new server.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with a new G450 or G430 Branch Gateway.

The simplex main/survivable core template supports Utility Services.

You require a new license for Communication Manager.

Preupgrade tasks

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Prerequisites

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server

or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

- To log 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`.
- To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, 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)**

     iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

     iv. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You

must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Verifying the hardware on the server

Before you begin

Log on to System Management Interface.

About this task

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.
   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:

Comments? infodev@avaya.com

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**.

4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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.

Upgrade tasks

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.

b. Log in to System Domain (Domain-0) as administrator.
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 administrator.
   c. In the command line, type **ip_forwarding disable** and press **Enter**.

      An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

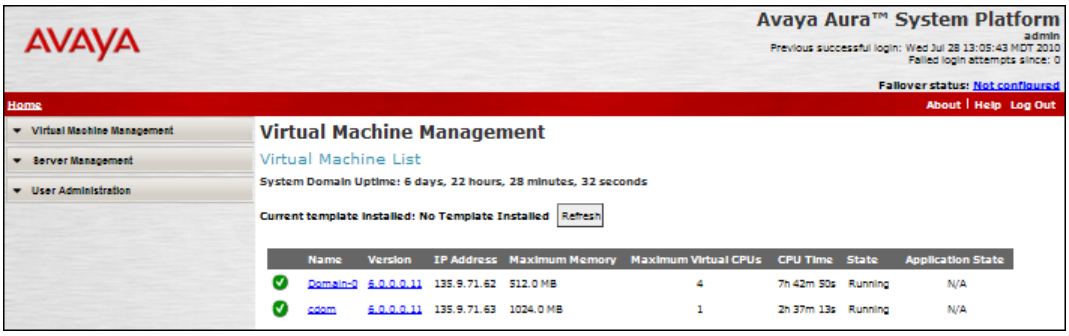
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**

- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:

a. Log on to System Management Interface.
b. On the **Administration** menu, click **Server (Maintenance)**.
c. Click **Server** > **Process Status**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrading DEFINITY SI or R Server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the following servers to Communication Manager Release 6.2 on an HP DL360 G7 Server or Dell 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 HP DL360 G7 Server or Dell 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 6.2 on the new server.
- Administering IPSIs on Communication Manager Release 6.2.
- 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 6.2.

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: - HP DL360 G7 - Dell R610 • 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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

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

Before you begin

A cross-over cable to connect your services laptop directly to the processor.

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Procedure

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

Procedure

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, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*
- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

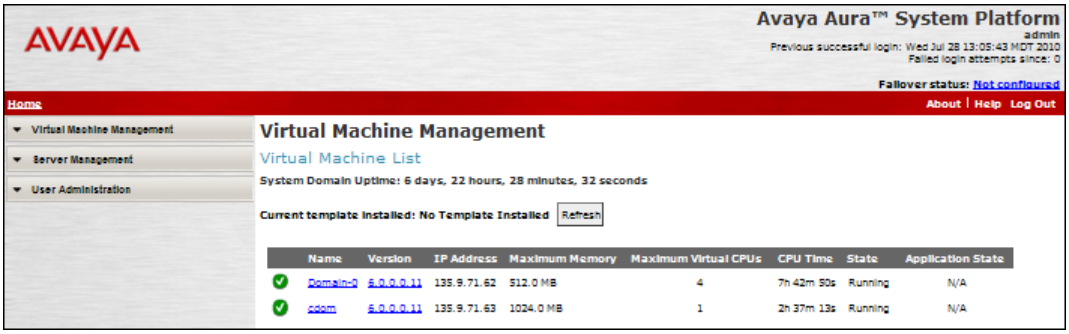
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.

- To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.

6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the 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 pack

Before you begin

Start a SAT session.

About this task

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

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 in the **Circuit Packs Available for Synchronization** section.
5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for 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 all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display PASS in the **Results** field. If the **Results** field does not display PASS, troubleshoot the synchronization error.

Completion tasks on the cabinet

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

About this task

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

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 HP DL360 G7 Server or a Dell R610 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 load balance across the IPSIs throughout the port networks.

Removing the processor port network control cabinet

About this task

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

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 if you want 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

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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 the HP DL360 G7 or Dell R610 Server

Introduction

Use this procedure to upgrade S8500A simplex server running Communication Manager releases 2.0 through 3.x to Release 6.2.1 on HP DL360 G7 Servers or Dell R610 Servers. The complete list of releases in this range is available at www.support.avaya.com.

In this procedure, you replace the S8500A Server by a pair of HP DL360 G7 Servers or Dell R610 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 a new server that supports Release 4.0.5 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 6.2.1 servers.
- Installing System Platform and Communication Manager duplex main/survivable core template on both the new servers that support Release 6.2.1.
- 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 new simplex server to both the new 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 6.2.1.

Use this section to upgrade Communication Manager from releases 2.0 through 3.x to Release 6.2.1:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on 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 6.2 template	

Documentation checklist

You need the following additional documentation:

✔	Task	Description
	Obtain one of the following as appropriate: • *Installing the HP DL360 G7 Server* (03-603799) • *Installing the Dell R610 Server* (03-603793)	Provides instructions for installing the 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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Preupgrade tasks on the S8500A Server

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:

a. Right-click and select **Paste**.

   The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.

    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

Before you begin

To use Telnet, enable the Telnet service for Communication Manager.

About this task

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

Procedure

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, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, 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

Procedure

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)

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up the files to a flashcard

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **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, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter 3.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.

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

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     i. Click **Specify Data Sets**.
     ii. Select the check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.
   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
6. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**
7. Click **Start Backup**.
8. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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)

About this task

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

Procedure

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

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

   You can select four files at a time.
6. 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 service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new 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

Before you begin

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

About this task

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.

Procedure

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

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`, where, *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name.
   The 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* indicates that a process has not started and you must investigate the reason before you proceed with the next upgrade step.
12. Close the Telnet session.

Installing service pack

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

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 a flashcard

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **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, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter 3.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up files to localhost

Before you begin

Enable the FTP service.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, 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. In the **Backup Method** section, 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 file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services laptop computer using FTP

About this task

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.

3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name 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 portable computer from the server

Procedure

Disconnect the services portable 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 a new server that supports Release 4.0.5

New server that supports Release 4.0.5

Complete the upgrade procedures described in the following sections on a new server that supports Communication Manager Release 4.0.5. For example, S8500 B or S8500C. At this point, you turn on the new server but you do not connect to the network.

Installing Communication Manager

Use this procedure to install Communication Manager Release 4.0.5 or Release 5.2.

Before you begin

- Install the new server, which supports Communication Manager release you want to install, in the rack.
- Insert the CD-ROM for Communication Manager Release 5.2.1 or Release 4.0.5 into the drive of the server.
- Turn on the server.

Procedure

1. On the portable computer, 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

Procedure

1. On the computer, 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 option 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

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

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

Copying files to the server

Before you begin

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

About this task

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`

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

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

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Creating a super-user login

About this task

Note:

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

Procedure

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

About this task

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 153.

Procedure

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. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `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

Before you begin

- Log on to System Management Interface.
- 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.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. 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**.
4. Click **View**.
5. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
6. Select both **Force** options.
7. Click **Restore**.
8. 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

About this task

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.

Procedure

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 computer to the server

Before you begin

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

About this task

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

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

Procedure

1. Disconnect the laptop from the Ethernet port labeled **2**.

2. Connect the laptop to the Ethernet port labeled **4**.

Accessing System Management Interface

About this task

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

Procedure

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

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.

3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up files to localhost

Before you begin

Enable the FTP service.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. In the **Data Sets** section, 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. In the **Backup Method** section, 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 file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services portable computer using FTP

About this task

Log on to the services portable computer.

Procedure

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

   Note the name of the directory, you need the name 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer 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 HP DL360 G7 or Dell R610 (Release 6.2.1) Server

Turning on the server

Before you begin

Do not connect the server to the network.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

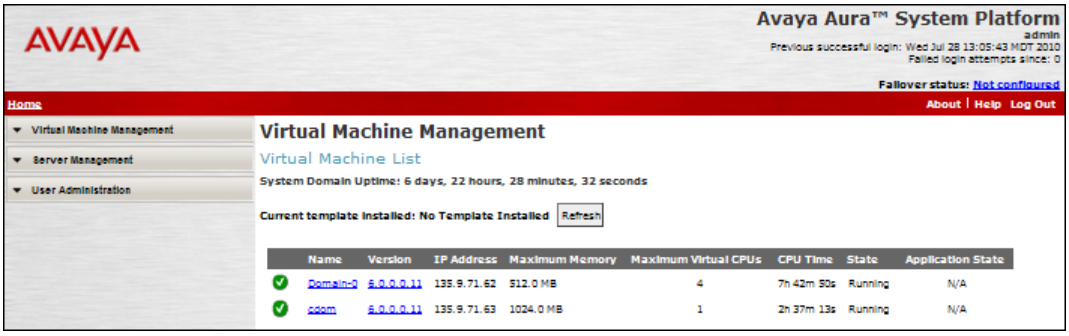
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Before you begin

Log on to System Management Interface.

About this task

Use this procedure to copy the service packs or the upgrade data set to the server, for example, `migration-60*.tar.gz` file.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

   You can select four files at a time.
6. 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 new simplex server to both the new servers.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the active S8500A Server

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Important:

Service outage begins at this point of the upgrade process.

Postupgrade tasks on the first HP DL360 G7 or Dell R610 (Release 6.2.1) active server

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.

7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Upgrade tasks on the second HP DL360 G7 or Dell R610 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

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

- Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

  Note:

  Do not install the Communication Manager license file when you upgrade a survivable remote 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

Procedure

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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

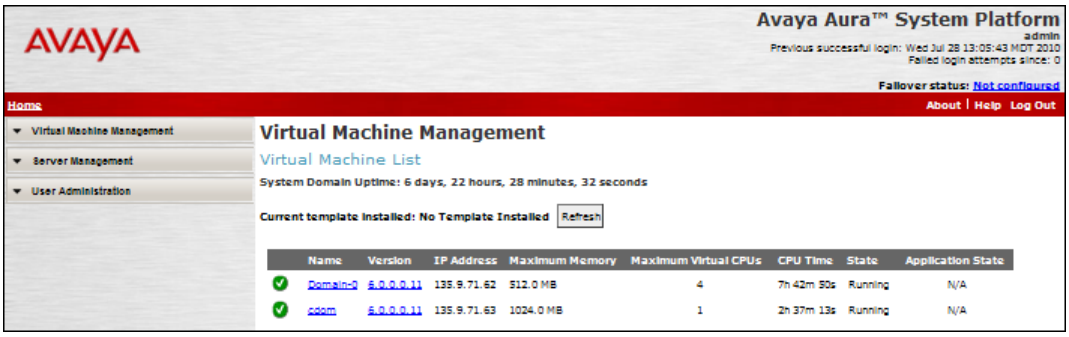
   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.
   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the connection for server duplication

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.
   If the two endpoints are connected, the system displays the message `MessRecv: 1`.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8500B or S8500C Server to HP DL360 G7 or Dell R610 Server

Introduction

Use this procedure to upgrade S8500B or S8500C simplex server running Communication Manager Release 4.0.5 or Release 5.2.1 to HP DL360 G7 Servers or Dell R610 Servers running Release 6.2.1.

In this upgrade procedure, you replace the S8500B or S8500C simplex server with HP DL360 G7 Servers or Dell R610 Servers running System Platform and the duplex main/survivable core template.

Duplex main/survivable core template on Communication Manager Release 6.x does not support Communication Manager Messaging.

Important:

If the S8500B or S8500C Server has Communication Manager Messaging installed on it, after the upgrade, messaging is not available on the system. To have messaging on your upgraded system, 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 6.2.1.

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 6.2.1.

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 6.2.1.
3. Perform the upgrade to Release 6.2.1 as described in this section.

Note:

You restore the upgrade dataset backed up from the existing server to both the new servers.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.2.1:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
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 S8500B or S8500C Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.

   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.

   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**

- **Host Name**
- **Directory**

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

4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Installing 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 Dell R610 Server, see *Installing the Dell™ PowerEdge™ R610 Server*.
- For HP DL360 G7 Server, see *Installing the HP ProLiant DL360 G7 Server*.

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 Appendix C on page 1679 for the worksheet to use for configuring the server.

Upgrade tasks on the first HP DL360 G7 or Dell R610 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, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

c. In the command line, type **ip_forwarding disable** and press **Enter**.

An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

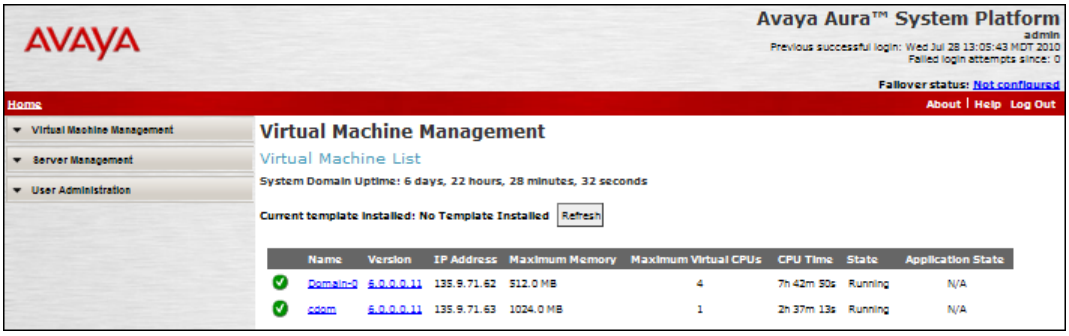
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.
   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the active S8500 Server

Shutdown the active S8500 Server as outlined in the following procedure and connect the first HP DL360 G7 Server or Dell R610 Server to the network.

Important:

After you shutdown the active S8500 Server, at this point, the service is nonfunctional. To minimize this time, shut down the active S8500 Server, access the first HP DL360 G7 Server or Dell R610Server again and release the server in the shortest amount of time possible.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the server from the rack

Procedure

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 HP DL360 G7 or Dell R610 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.

5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Upgrade tasks on the second HP DL360 G7 or Dell R610 Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

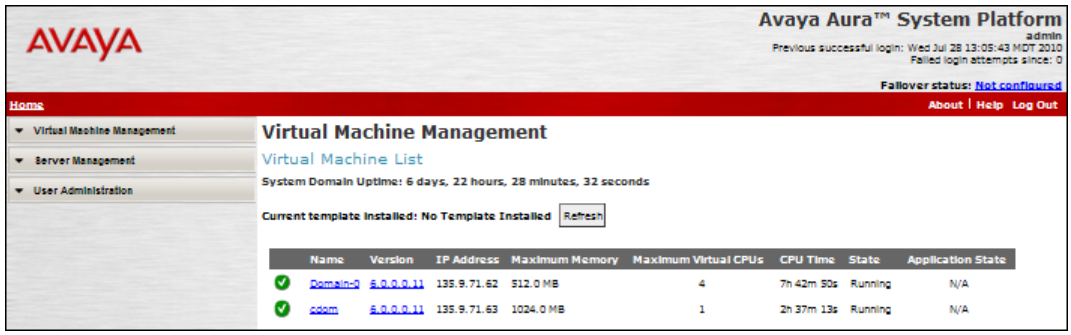
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory ***/vsp-template***:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8510 server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade S8510 simplex server running Communication Manager Release 5.2.1 to HP DL360 G7 Servers or Dell R610 Servers running Release 6.2.1.

In this upgrade procedure, you replace the S8510 simplex server with HP DL360 G7 Servers or Dell R610 Servers running System Platform and the duplex main/survivable core template.

Duplex main/survivable core template on Communication Manager Release 6.x does not support Communication Manager Messaging.

Important:

If Communication Manager Messaging is installed on the S8510 Server, after the upgrade, messaging is not available on the system. To have messaging on your upgraded system, 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 6.2.1.

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 6.2.1.

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 6.2.1.
3. Perform the upgrade to Release 6.2.1 as described in this section.

Note:

You restore the upgrade dataset backed up from the existing server to both the new servers.

Use this section to upgrade Communication Manager from Release 5.2.1 to Release 6.2.1 on:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://

support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
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 S8510 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**

- **Host Name**
- **Directory**

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

4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Installing 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 Dell R610 Server, see *Installing the Dell™ PowerEdge™ R610 Server*.
- For HP DL360 G7 Server, see *Installing the HP ProLiant DL360 G7 Server*.

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 Appendix C on page 1679 for the worksheet to use for configuring the server.

Upgrade tasks on the first HP DL360 G7 or Dell R610 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, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

c. In the command line, type **ip_forwarding disable** and press **Enter**.

An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

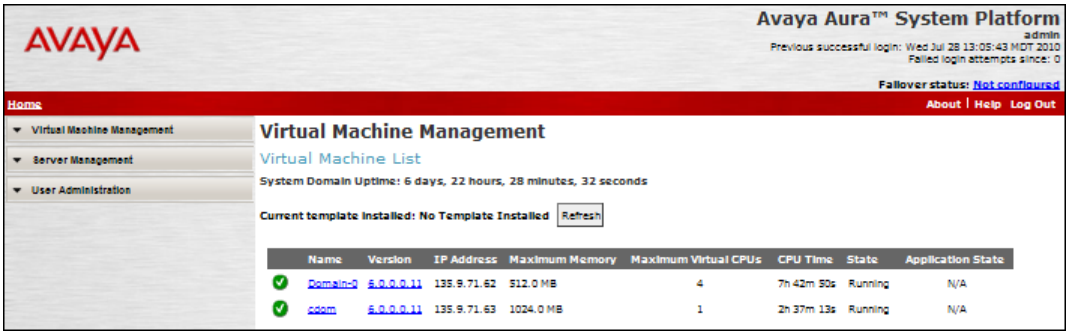
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:

   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

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 system is out of service as the S8510 Server is shutdown. To minimize this time, shut down the S8510 Server, access the first HP DL360 G7 Server or Dell R610 Server again and release the server immediately.

You must continue to perform upgrade procedures on the first HP DL360 G7 Server or Dell R610 Server.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the server from the rack

Procedure

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 HP DL360 G7 or Dell R610 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay

4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Upgrade tasks on the second HP DL360 G7 or Dell R610 Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

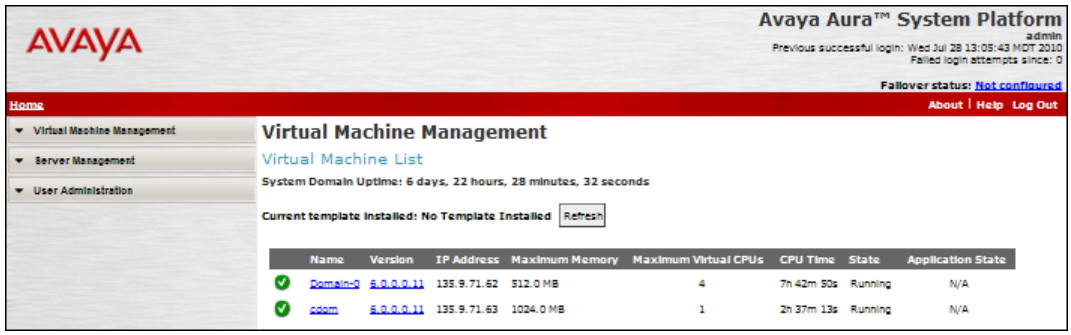
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8700-Series Servers to the HP DL360 G7 or Dell R610 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 HP DL360 G7 Servers or Dell R610 Servers.
2. Release 5.x on S8700–Series Servers, which are not connected to the network, to Release 5.2.1 on HP DL360 G7 Servers or Dell R610 Servers.
3. Release 5.2.1 on S8800 Servers to Release 6.2.1 on HP DL360 G7 Servers or Dell R610 Servers, which you connect to the network only later during this upgrade step.
4. Release 5.2.1 on S8800 Servers to Release 6.2.1 on S8800 Servers, which you connect to the network only later during this upgrade step.

In this upgrade procedure, you replace the S8700–Series Servers with HP DL360 G7 Servers or Dell R610 Servers running System Platform and the duplex main/survivable template (CM_Duplex).

Convert the fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1697.

- 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.

Related topics:

S8700 Server upgrade procedure on page 750
High-level tasks on page 750

S8700 Server upgrade procedure

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 procedure outlined in this section.

Use the following procedures for each S8700-Series Server to upgrade to Release 4.0.5 or 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)	-

High-level tasks

Perform the following high-level tasks to upgrade the system:

- 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 the new servers and restoring the backed up data from the existing servers.

- 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 6.2.
- Installing System Platform and Communication Manager on both the new 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 6.2.

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks on the active S8700 Server

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.

4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

Before you begin

To use Telnet, enable the Telnet service for Communication Manager.

About this task

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

Procedure

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, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, 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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     i. Click **Specify Data Sets**.
     ii. Select the check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.
   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
6. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**
7. Click **Start Backup**.
8. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

9. Select the backup file from the list and click **Check Status**.

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

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Converting fiber PNs to IP-PNC

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1697.

Note:

For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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)

About this task

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

Procedure

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

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

You can select four files at a time.

6. 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 service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new 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

Before you begin

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

About this task

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.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.
   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`, where *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name. .
   The 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. To view the status of the processes, enter `statapp -c`.
    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

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.

3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

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 a flashcard

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **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, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter 3.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up files to localhost

Before you begin

Enable the FTP service.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, 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. In the **Backup Method** section, 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 file from the list and click **Check Status**.

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

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services laptop computer using FTP

About this task

Log on to the services laptop computer.

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.

3. Enter `cd <directory name>`, to navigate to the directory, where you save the backup file.

   Note the name of the directory, you need the name 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 portable computer from the server

Procedure

Disconnect the services portable 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

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.
    c. Enter `almsnmpconf` and record the output.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**

- **SAT (Telnet 5023)**

4. Click **Submit**.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - Click **Full Backup**.
   - If Communication Manager is on release 1.x, 2.0 or 2.0.1:
     i. Click **Specify Data Sets**.
     ii. Select the check boxes:
     - **Avaya Call Processing (ACP) Translations**
     - **Server and System Files**
     - **Security Files**
4. In the **Download size** field, enter the size of the backup `.tar` file.
   If the backup file size is large, there may be more than one `.tar` file.

5. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
6. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**
7. Click **Start Backup**.
8. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

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

4. Click **Browse** to open the **Choose File** window on your computer.

5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. 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 service packs to upgrade S8500A Server running Communication Manager Release 2.x to Release 4.0.5 on the new 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

Before you begin

- Obtain the latest service pack for the currently running Communication Manager release and activate it.

About this task

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.

Procedure

1. Click **Start** > **Run**.
2. Enter `telnet 192.11.13.6`.
3. Log in as `craft` or `dadmin`.
4. To access the `ftp` directory, enter `cd /var/home/ftp`.
5. To list the files in the `ftp` directory, at the prompt, enter `ls -ltr`.
   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`, where *patch* is the release or issue number of the service pack file, for example, 03.1.526.5-1003. Do not use the `*.tar.gz` extension at the end of the file name. .
   The 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. To view the status of the processes, enter `statapp -c`.
    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

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

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 a flashcard

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, perform one of the following:
   - For Communication Manager releases earlier than 3.0, click **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, click **Full Backup**.
4. In **Backup Method** section, click **Local PC card**.
5. In the **Retain** field, enter 3.
6. Click **Start Backup**.
7. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up files to localhost

Before you begin

Enable the FTP service.

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, 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. In the **Backup Method** section, 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 file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services laptop computer using FTP

About this task

Log on to the services laptop computer.

Procedure

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

   Note the name of the directory, you need the name 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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Preparing the new servers for the upgrade

- Install both the staged servers to the data equipment rack. The new servers can be one of the following:
  - HP DL360 G7 Server

    For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*
  - Dell R610 Server.

    For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.
- Connect both the servers to the power supply. Do not turn on the servers.
- Do not connect the servers to any network until instructed.
- Do not connect the server duplication cable until instructed.

Complete the upgrade procedures on the staged servers.

Complete the procedures starting from Inserting the CD for Communication Manager CD on page 777 through Completion tasks on the staged server on page 788 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 the Communication Manager disc

Procedure

1. Open the CD-ROM drive on the server.

2. Insert the disc for Communication Manager software in the CD/DVD drive and close the drive.

Turning on the server

Procedure

1. Plug one end of the power cord into the socket at the back of the power supply and the other end into a UPS or nonswitched outlet.

   Approximately 5 seconds after you connect the server to the power supply, one or more fans might start to provide cooling, and the power-on LED blinks quickly at three flashes per second. About 30 seconds after you turn on the server, the power-on LED blinks slowly at one flash per second, and one or more fans might provide cooling.

   Note:

   Wait for the power-on LED to blink slowly before you press the power button. If you press the power button while the power-on LED blinks quickly, the server does not turn on.

2. Press the power button on the front of the server.

   When the Green power-on LED on the server 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 unavailable, or the power supply or the LED itself has failed.
   - Flashing rapidly: The server is turned off and is not ready to be turned on. The power-control button is disabled. This state lasts for about 30 seconds.
   - Flashing slowly: 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:

   Do not connect the new 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

Procedure

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**.
3. In the Run dialog box, 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

Before you begin

Insert the CD-ROM for Communication Manager Release 5.2.1 or Release 4.0.5 into the drive of the server.

Procedure

1. On the portable computer, 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

Procedure

1. On the computer, 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 option 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

About this task

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

Procedure

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

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. 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

Before you begin

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

About this task

Use the steps described in this section to download the following files:

- The latest available service pack for Communication Manager Release 5.2.1
- The license for Communication Manager Release 5.2.1
- The Avaya authentication file for Communication Manager Release 5.2.1
- The 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Verifying the process status

Procedure

1. In the navigation pane, click **Server** > **Process Status**.
2. In the **Frequency** section, click `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

Before you begin

Log on to System Management Interface.

Procedure

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

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Creating a super-user login

About this task

Note:

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

Procedure

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

About this task

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 153.

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.`

Procedure

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. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `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

Before you begin

- Log on to System Management Interface.
- 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.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. 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**.
4. Click **View**.
5. Select the file to restore, for example, `full_cmserver1_*.tar.gz`.
6. Select both **Force** options.
7. Click **Restore**.
8. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Shutdown Server**.
3. Select the following check boxes:
   - **Restart server after shutdown**
   - **Shutdown even if this is the active server**
4. Click **Shutdown**.
   The system displays the `A server shutdown has been requested` message.

Completion tasks on the staged server

Procedure

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

Before you begin

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

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. Select the **SSH** protocol.

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 host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.

2. Enter `192.11.13.6`.
   You will be logged into the server.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Identifying the Ethernet interface

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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.

   The interface assigned does not persist throughout the process to upgrade to Release 6.0.x. However, you must know the Ethernet interface assigned to complete the staging of the servers on Communication Manager Release 5.2.1.

Connecting the server duplication cable to the first staged server

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify that `Mode` is `Active`.

   If the `Mode` is `BUSY OUT`, release the server. The server goes to the `Active` mode.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Completion tasks on the staged server

Procedure

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

Before you begin

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

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. Select the **SSH** protocol.
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 host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing System Management Interface

About this task

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

Procedure

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

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying system status

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify that `Mode` is `BUSY OUT`.
4. 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.
5. Repeat steps 2 through 4 to verify if the `Mode` is `BUSY OUT`.

Identifying the Ethernet interface

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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.

The interface assigned does not persist throughout the process to upgrade to Release 6.0.x. However, you must know the Ethernet interface assigned to complete the staging of the servers on Communication Manager Release 5.2.1.

Connecting the server duplication cable to second staged server

Before you begin

One end of the Ethernet cable connected to the first server.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.
   If the two endpoints are connected, the system displays the message `MessRecv: 1`.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

At this point, the first server is active mode and the second server is busied out.

Completion tasks on the staged server

Procedure

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

Before you begin

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

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. Select the **SSH** protocol.
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 host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Starting a SAT session

Before you begin

Log on to the services port from a directly connected laptop.

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, 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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, 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

Perform the procedures starting from Installing the preupgrade service packs on page 157 through Completing duplication cable connections on staged servers on page 803 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

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Enabling FTP service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. On the Server Access page, for the **FTP Server** field, click **Enable**.
   The system enables the FTP service on the local server. The FTP service remains enabled for 15 minutes and automatically gets disabled.
4. Click **Submit**.

Backing up the files to localhost

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. 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`.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Transferring files to the services portable computer using FTP

About this task

Log on to the services portable computer.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Completing duplication cable connections on staged servers

Procedure

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 new (Release 6.2.1) servers

Complete the procedures starting from Installing System Platform and Communication Manager on page 194 through Rebooting the server on page 168 on the first staged server running Communication Manager Release 6.2 first. Repeat the procedures on the second staged server running Communication Manager Release 6.2.

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Connecting the cables to the new server

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

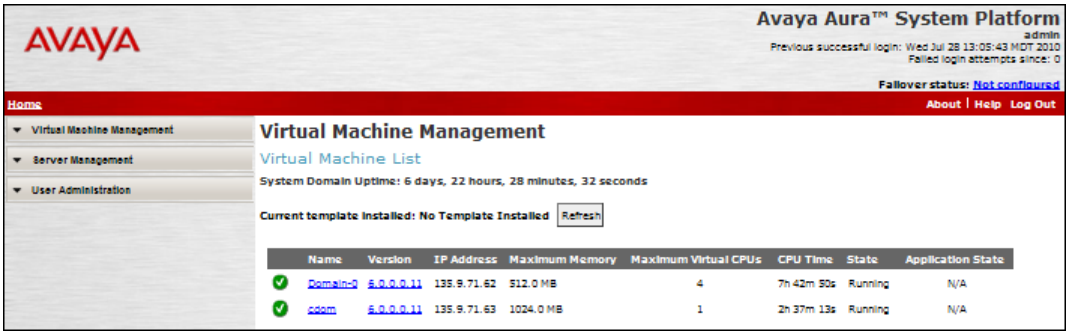
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Before you begin

Log on to System Management Interface.

About this task

Use this procedure to copy the service packs or the upgrade data set to the server, for example, `migration-60*.tar.gz` file.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verification tasks on the staged servers running Release 6.2.1

Starting a SAT session

Before you begin

Log on to the services port from a directly connected laptop.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Verification tasks on the first staged active (Release 6.2.1) server

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the connection for server duplication

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.

4. Click **Execute Ping**.
   If the two endpoints are connected, the system displays the message `MessRecv`: 1.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   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

Before you begin

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

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. Select the **SSH** protocol.
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 host key of the server.
   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.

9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.
2. In the browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

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

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Completion tasks on the active S8700 Server

Connecting a laptop to the server

Before you begin

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

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. Select the **SSH** protocol.
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 host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**

2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.
2. In the browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

   - LAN access by host name

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

   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Important:

Service outage begins at this point of the upgrade process.

Postupgrade tasks on the first staged Release 6.2.1 active server

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Postupgrade tasks on the second staged Release 6.2.1 server (busied out)

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8700-Series servers to the HP DL360 G7 or Dell R610 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 6.2.1 on HP DL360 G7 Servers or Dell R610 Servers.

In this upgrade procedure, you replace the S8700-Series servers with HP DL360 G7 Servers or Dell R610 Servers running System Platform and the duplex main/survivable core template (CM_Duplex).

Note:

From Release 6.0.1 onwards, Communication Manager supports upgrading to HP DL360 G7 Servers or Dell R610 Servers.

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1697.

- 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 6.2.1.

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 6.2.1.

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 6.2.1.
3. Perform the upgrade to Release 6.2.1 as described in this section.

Use this section to upgrade Communication Manager from Release 4.0.5 or Release 5.2.1 to Release 6.2.1:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the 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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
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

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Converting fiber PNs to IP-PNC

You must convert fiber port network connectivity (PNC) to IP-PNC. For instructions to convert, see Converting from fiber port networks to IP-PNC on page 1697.

Note:

For Communication Manager releases earlier than 3.0, perform the conversion after you upgrade the servers.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Preupgrade tasks on the standby S8700-Series Server

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.

2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the 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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... unpacked successfully`.
   - If the status of the update file you want to activate is `unpacked`:

Comments? infodev@avaya.com

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**.

4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the duplication cable

Procedure

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

Procedure

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 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 Dell R610 Server, see *Installing the Dell™ PowerEdge™ R610 Server*.
- For HP DL360 G7 Server, see *Installing the HP ProLiant DL360 G7 Server*.

Upgrade tasks on the first HP DL360 G7 or Dell R610 Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

Procedure

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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

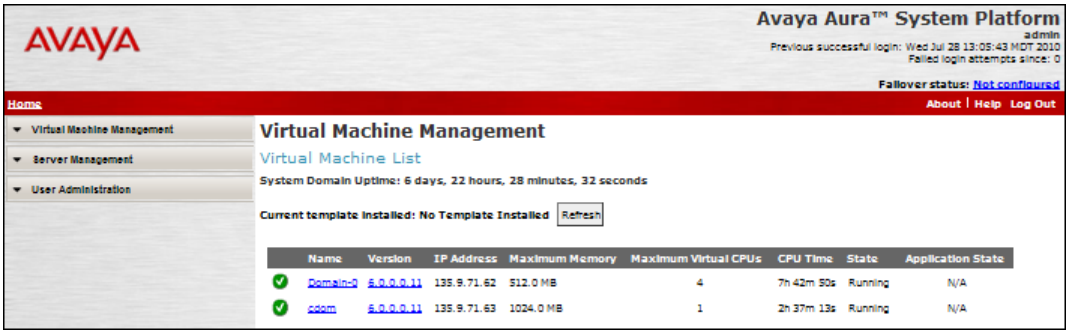
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying connectivity

About this task

To verify if the Ethernet port is working, ping the FTP server, where you saved the backup files.

Procedure

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).

Completion tasks on the active S8700 Server

Perform the following two procedures on the active S8700 Server.

Important:

After you complete the two mentioned tasks, at this point, the system is out of service as both the S8700 servers are shutdown. To minimize this time, shut down the active S8700 Server, access the first HP DL360 G7 Server or Dell R610 Server and release the server immediately.

Continue with the upgrade procedures on the HP DL360 G7 Server or Dell R610 Server.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Removing the server from the rack

Procedure

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 HP DL360 G7 or Dell R610 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.
2. Open a Web browser and log onto the server using System Management Interface.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.

3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Upgrade tasks on the second HP DL360 G7 or Dell R610 Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

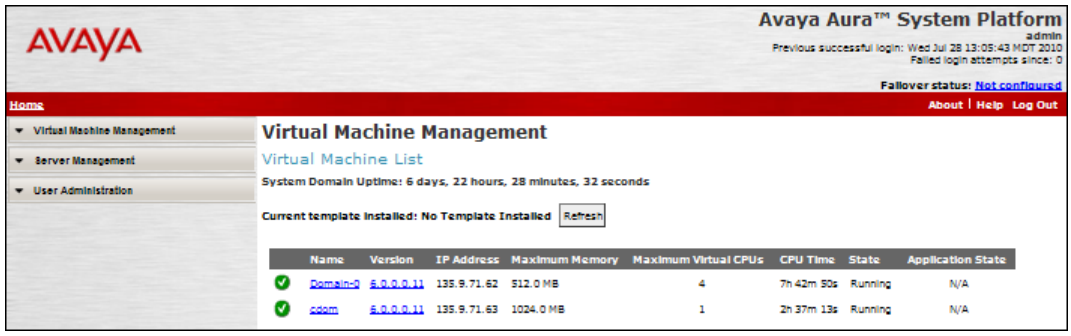
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2.1 using System Platform and the duplex main/survivable template on 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 6.2.1.

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 6.2.1.

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 6.2.1 from the Avaya Support website 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)

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the 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-ROM to update the uEFI firmware using one of the following ways: • Order the *uEFI firmware* CD-ROM • Download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CD-ROM.	
	Obtain the *RIAD 5 firmware* CD-ROM	
	Obtain the CD-ROM to update the uEFI settings using one of the following ways: • Order the *uEFI settings* CD-ROM • Download the `S8800uEFITool.iso` file	

✔	Task	Description
	from Avaya Support Site and create a CD-ROM.	
	Download the instructions for updating the uEFI firmware and uEFI settings from the Avaya Support Site.	

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
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

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.

2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
3. In the **Download size** field, enter the size of the backup `.tar` file.
   If the backup file size is large, there may be more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

About this task

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.
   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server

or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the 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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

3. In the **Data Sets** section, 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)**

     iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

     iv. In the **Download size** field, enter the size of the backup `.tar` file.

     If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You

must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

About this task

Verify the memory, hard disk drive, and RAID configuration on the existing server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Display Configuration**.
   The system opens the Display Configuration page.
3. In the **Disk devices** field, verify whether the system has three 146 GB hard disk drives. If the system does not have three hard disk drives, install a hard disk drive on the server later in the upgrade process or when the system prompts you to install.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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

Before you begin

Before you disconnect the server from the power source, note which LEDs are lit, including the LEDs that are lit on the operation information panel and 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 do not light up when the power source is removed.

About this task

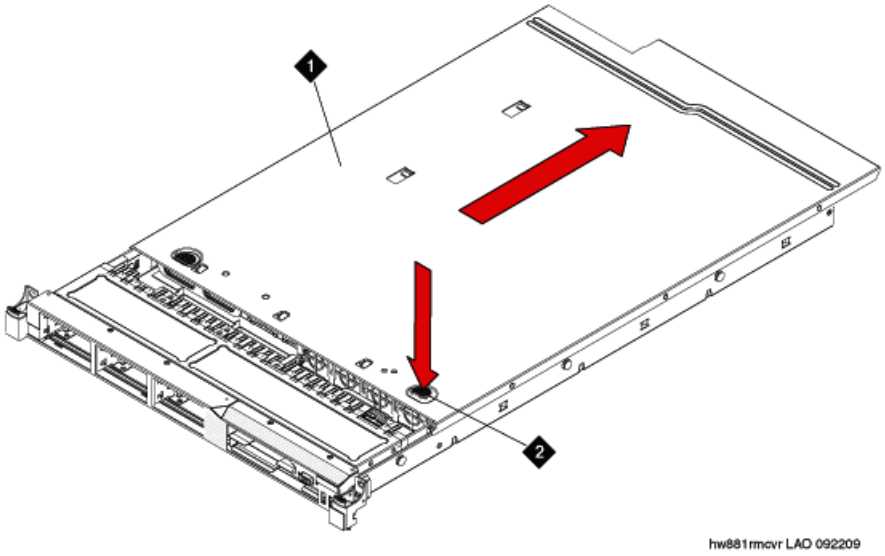
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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

About this task

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 a missing air baffle might damage server components.

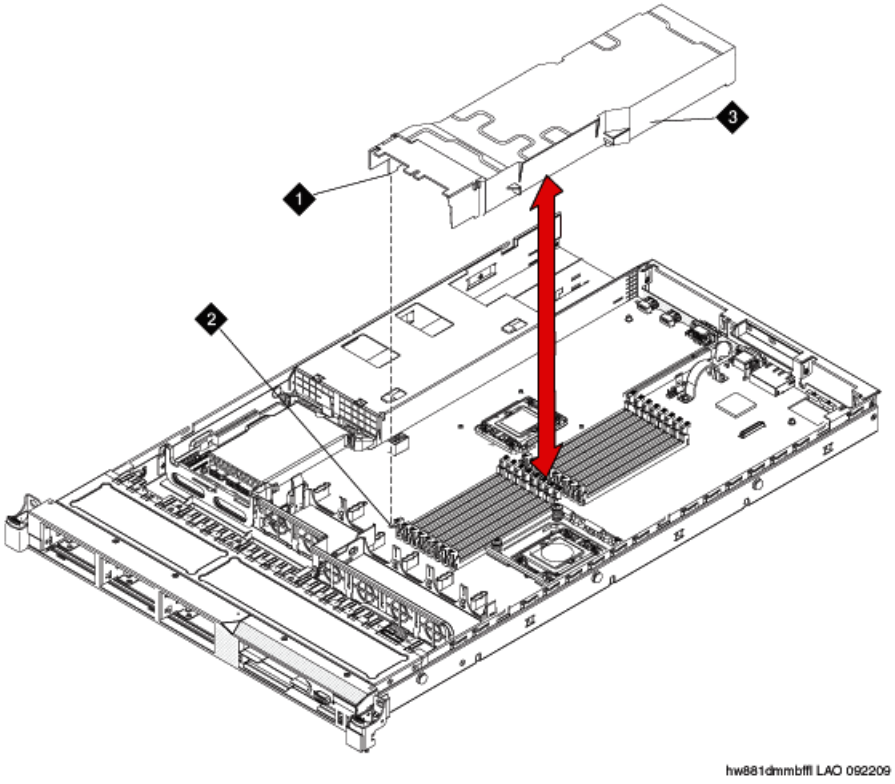
Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

1. Turn off the server and all attached devices.

2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM 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

Before you begin

Remove the DIMM air baffle.

About this task

Important:

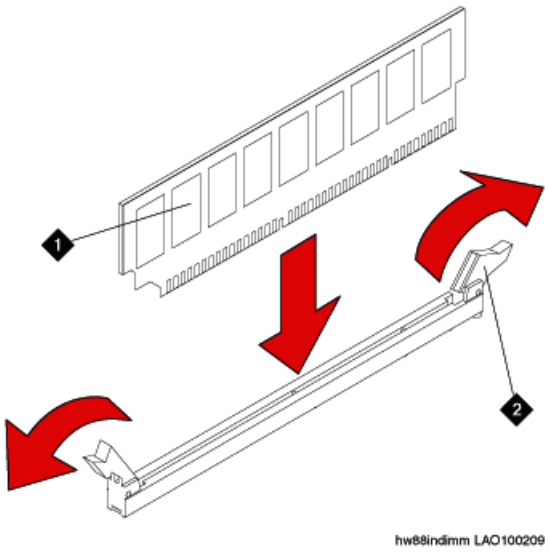
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

About this task

You must install the DIMM air baffle after you install a memory module.

Caution:

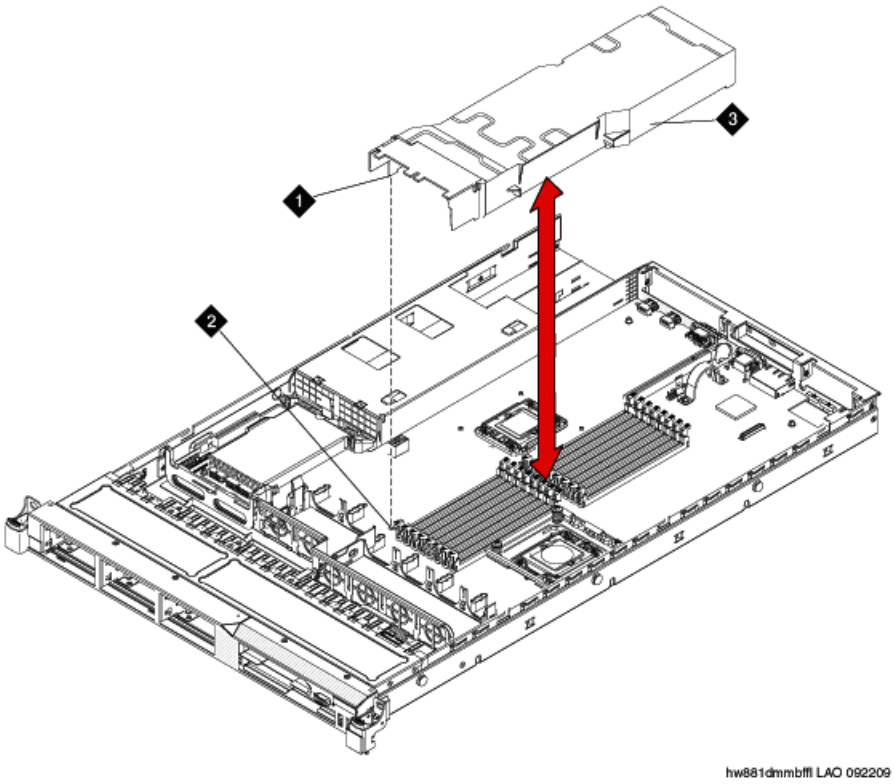
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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 the 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

Before you begin

If replacing an existing hard drive, remove the hard drive that you want to replace.

About this task

Important:

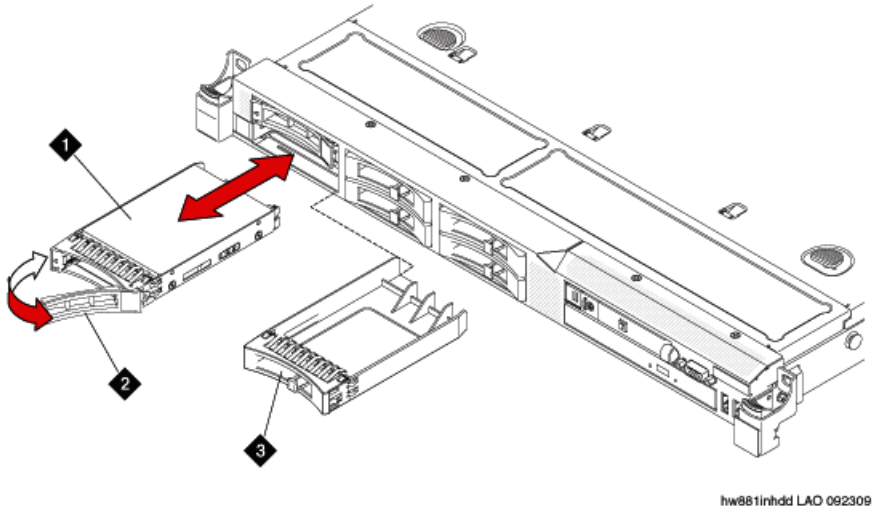
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

Before you begin

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Before you begin

- 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.

About this task

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.

Procedure

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

Before you begin

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Upgrade tasks on the standby server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

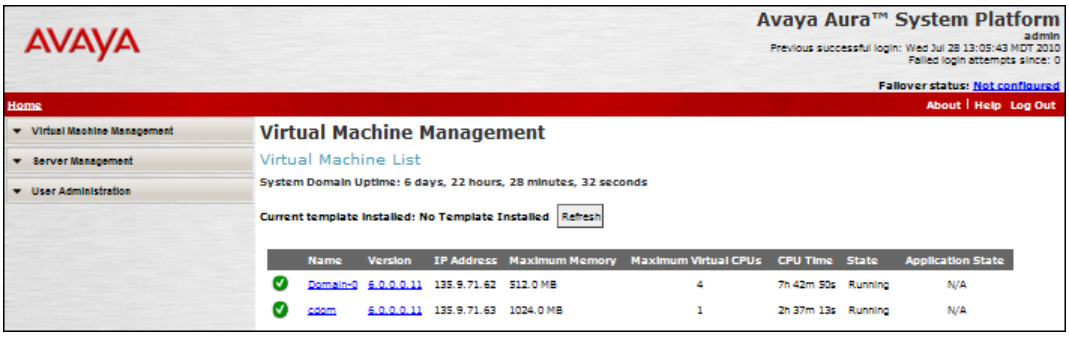
1. Open a compatible Internet browser on your computer.
   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.

8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Upgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrade tasks on the S8800 Server that is shutdown

Removing the server cover

Before you begin

Before you disconnect the server from the power source, note which LEDs are lit, including the LEDs that are lit on the operation information panel and 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 do not light up when the power source is removed.

About this task

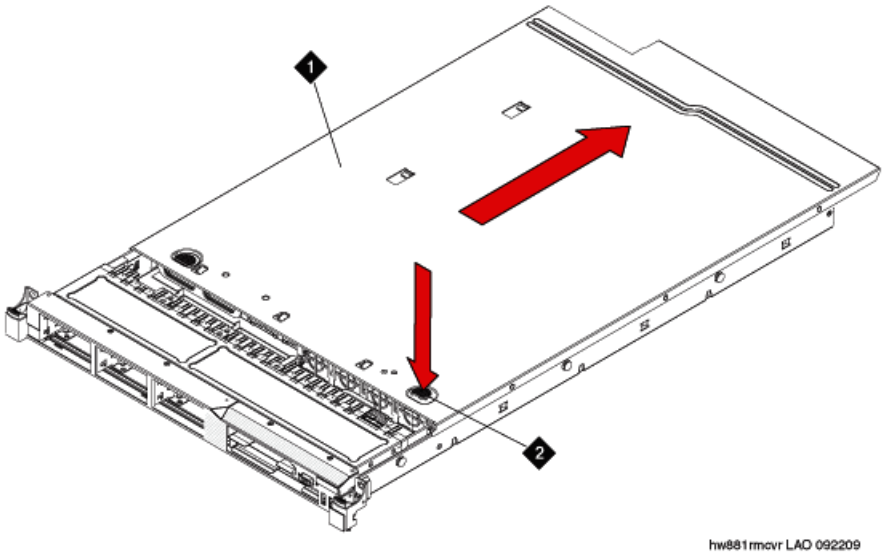
Remove the server cover to access the server's internal components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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

About this task

You must remove the DIMM air baffle to replace or install a memory module.

Caution:

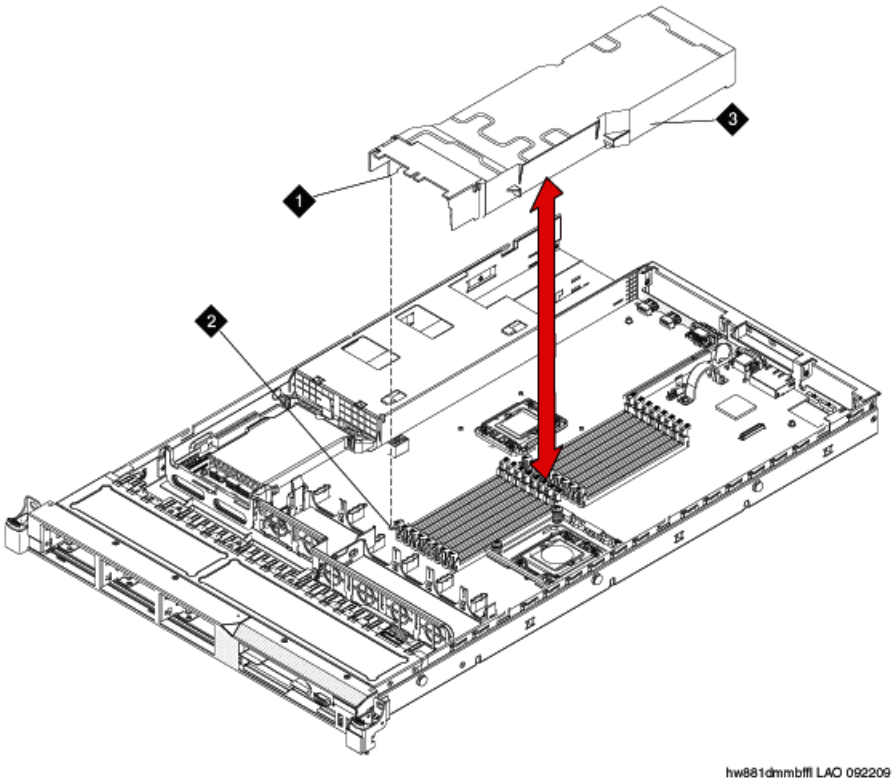
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Lift the DIMM 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

Before you begin

Remove the DIMM air baffle.

About this task

Important:

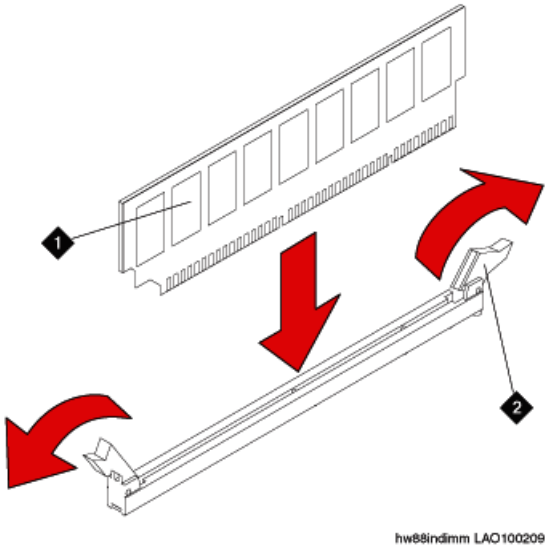
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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, if a monitor and keyboard are connected, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

About this task

You must install the DIMM air baffle after you install a memory module.

Caution:

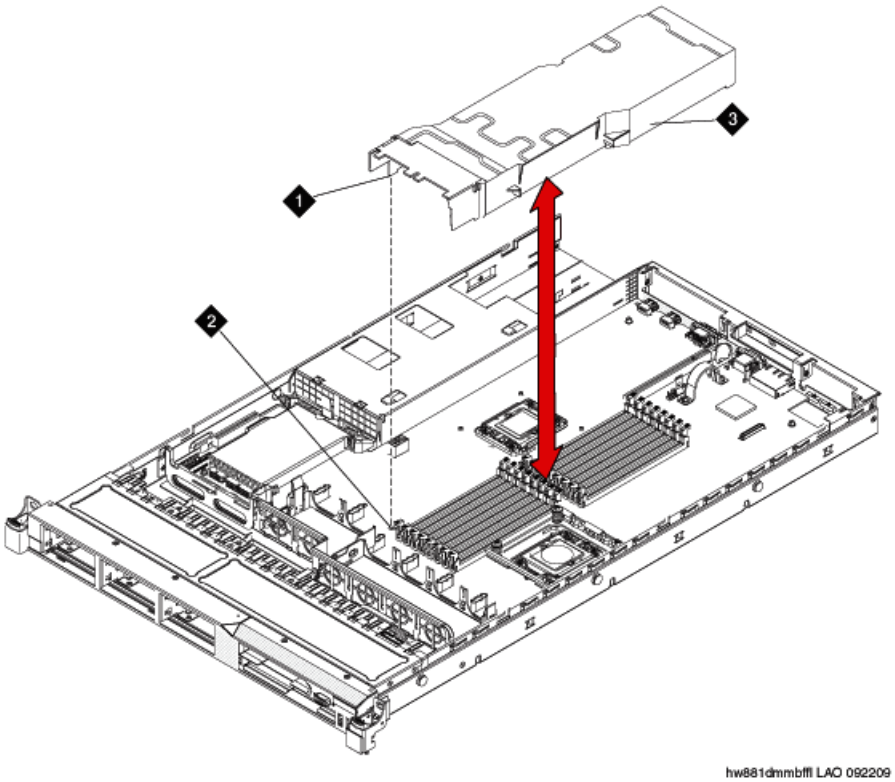
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with a missing air baffle might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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 the 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

Before you begin

If replacing an existing hard drive, remove the hard drive that you want to replace.

About this task

Important:

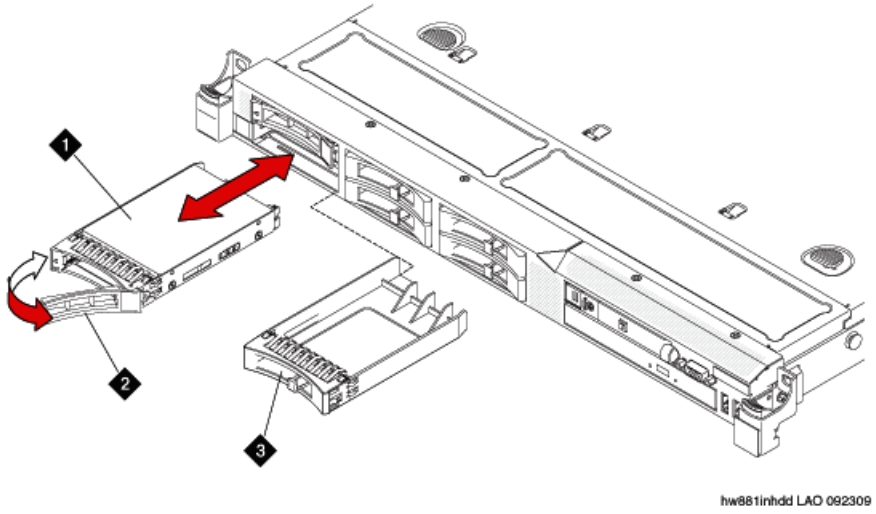
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. For more information, see Protecting against ESD damage.

Procedure

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. An amber LED that remains lit indicates a faulty drive that you must replace.

Updating S8800 server firmware

Before you begin

- Obtain the CO-ROM for uEFI firmware. You order the CO-ROM or download the `S8800firmwareupdates.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI firmware from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800firmwareupdates.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800firmwareupdates.iso` file on the server.

Converting the disk array to RAID 5

Before you begin

- 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.

About this task

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.

Procedure

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

Before you begin

- Obtain the CO-ROM for uEFI settings of S8800 Server. You order the CO-ROM or download the `S8800uEFITool.iso` file from Avaya Support Site and create a CO-ROM.
- Download the instructions for updating the uEFI settings from the Avaya Support Web site at http://support.avaya.com.

About this task

Important:

If you fail to install the `S8800uEFITool.iso` updates, the system generates unpredictable results with System Platform and Communication Manager.

Procedure

Install the `S8800uEFITool.iso` file on the server.

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Connecting the cables to the server

Procedure

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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain (Cdom).

Note:

- You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.
  - https://<*IP_Address*>
  - https://<*FQDN*>

    Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).
- This is a secure site. If you get a certificate error message, follow the instructions on 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

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Installing service pack

Before you begin

- Copy the latest service packs from the Avaya Support Site to the services portable computer.
- Log on to System Platform Web Console.

About this task

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.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the active server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.

3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

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

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the HP DL360 G7 Server to HP DL360 G7 Server on System Platform

Introduction

This section describes the procedure to upgrade Communication Manager from Release 5.2.1 on duplex HP DL360 G7 Servers to Release 6.2.1 using System Platform and the duplex main/survivable template on HP DL360 G7 Servers.

In this upgrade procedure, you:

- Reuse the HP DL360 G7 Server.
- Install System Platform and the duplex main/survivable template (CM_Duplex) on the existing servers.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with a new G450 or G430 Branch Gateway.

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 6.2.1.

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 6.2.1.

Use this section to upgrade:

- 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the required software: • System Platform • the required Communication Manager template	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server

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 HP DL360 G7 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:

- To log 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`.
- To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.

If the size of the backup file is large, you may have more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

Note:

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

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Procedure

1. Label and disconnect the power cords 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 HP DL360 G7 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the 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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.

2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.

3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

Procedure

1. Label and disconnect the power cords 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.

Upgrade tasks on the standby server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:

a. Start an SSH session.
b. Log in to System Domain (Domain-0) as administrator.
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 administrator.
   c. In the command line, type **ip_forwarding disable** and press **Enter**.

      An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

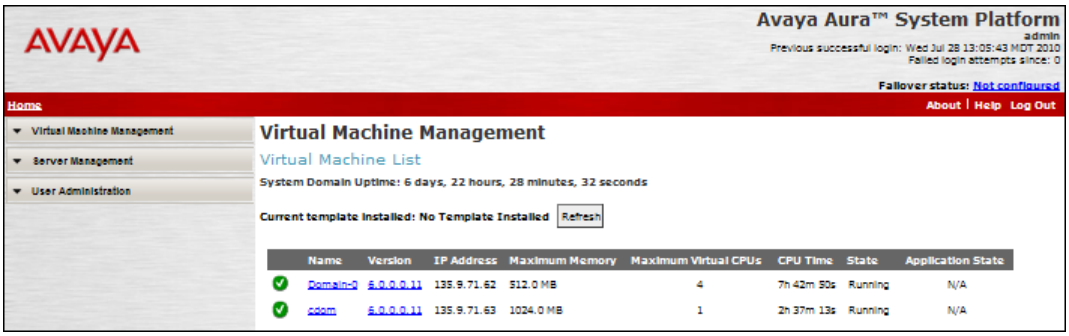
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**

- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.

6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Tasks on the active HP DL360 G7 Server

Completion tasks on the active HP DL360 G7 Server

When you shutdown the active HP DL360 G7 Server as outlined in the following procedure, the service outage begins.

Important:

To minimize the downtime, shut down the active server, access the standby server and release the server in the shortest amount of time possible.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Upgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Upgrade tasks on the server that is shutdown

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Connecting the cables to the server

Procedure

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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain (Cdom).

Note:

- You can connect using `http`, but you will be immediately redirected to `https`. Either of two https formats are acceptable for accessing Web Console administration pages.
  - https://<*IP_Address*>
  - https://<*FQDN*>

    Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).
- This is a secure site. If you get a certificate error message, follow the instructions on 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

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.

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

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the active server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on the standby server

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.

3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.

3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading the S8800 Server to HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade Communication Manager Release 5.2.1 on duplex S8800 Servers to Release 6.2.1 on HP DL360 G7 Servers or Dell R610 Servers.

In this upgrade procedure, you:

- Replace one of the following:
  - S8800 Server with an HP DL360 G7 Server or Dell R610 Server
  - HP DL360 G7 Server with a Dell R610 Server
- Install System Platform and the duplex main/survivable template (CM_Duplex) on the new servers.
- Reuse the existing G450, G430, G250, G350, G700, or G650 gateway or replace the gateway with a new G450 or G430 Branch Gateway.

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 6.2.1.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and some elements of the server configuration.

You require a new license for Communication Manager.

Presite preparation

Presite upgrade checklist

Before you go onsite, perform the following tasks:

✔	Task	Description
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Ensure that you remove private control networks for IPSI connectivity to the server before you run a preupgrade backup.	For instructions, see Introduction on page 1693.
	Ensure that you have the upgrade-specific hardware.	_
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
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

About this task

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

Procedure

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

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

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

Important:

Do not click **Submit**.

9. At 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 the product ID.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.

4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Checking for translation corruption

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Preupgrade tasks on the standby S8800 Server

Accessing the System Management Interface

About this task

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

Procedure

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

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**

- **Host Name**
- **Directory**

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

4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Installing 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 Dell R610 Server, see *Installing the Dell™ PowerEdge™ R610 Server*.
- For HP DL360 G7 Server, see *Installing the HP ProLiant DL360 G7 Server*.

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 Appendix C on page 1679 for the worksheet to use for configuring the server.

Upgrade tasks on the first HP DL360 G7 or Dell R610 Server

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

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

Procedure

1. Do not connect the server to the network until the procedure in this section instructs.
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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

c. In the command line, type **ip_forwarding disable** and press **Enter**.

An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

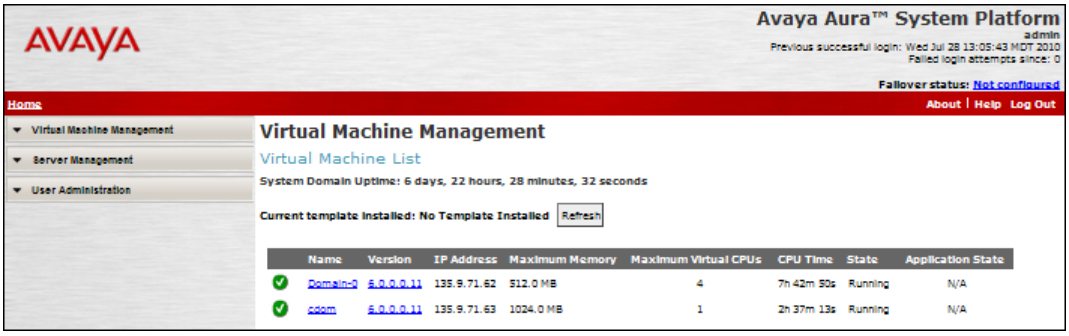
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to SMI 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, gain access to the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.
   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the 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 is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To 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 the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 the Logon page generates. 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 home page of the Communication Manager SMI.

Note:

You must restore the upgrade dataset backed up from the staged new simplex server to both the new servers.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on the active S8800 Server

Shutdown the active S8800 Server as outlined in the following procedure and connect the first HP DL360 G7 Server or Dell R610 Server to the network.

Important:

After you shutdown the active S8800 Server, at this point, the service is nonfunctional. To minimize this time, shut down the active S8800 Server, access the first HP DL360 G7 Server or Dell R610Server again and release the server in the shortest amount of time possible.

Shutdown tasks on S8800 Server

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.

6. Wait about 30 seconds before you perform the next step.

Disconnecting the cables

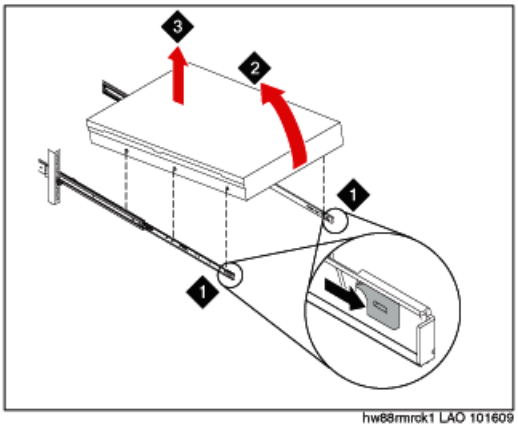
Procedure

1. Label and disconnect the power cords 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 from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.



4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

Postupgrade tasks on the first HP DL360 G7 or Dell R610 Server

Accessing the new server

Procedure

1. Clear the ARP cache on the portable computer, if necessary.

2. Open a Web browser and log onto the server using System Management Interface.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.

3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays:
   - `UP` for all operations
   - `Down` for `dupmgr`
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

About this task

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance on page 43.

Saving translations

About this task

Perform this procedure on the main server only.

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:

- To change the schedule backup, click **Change**.

  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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
- *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Upgrade tasks on the second HP DL360 G7 or Dell R610 Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

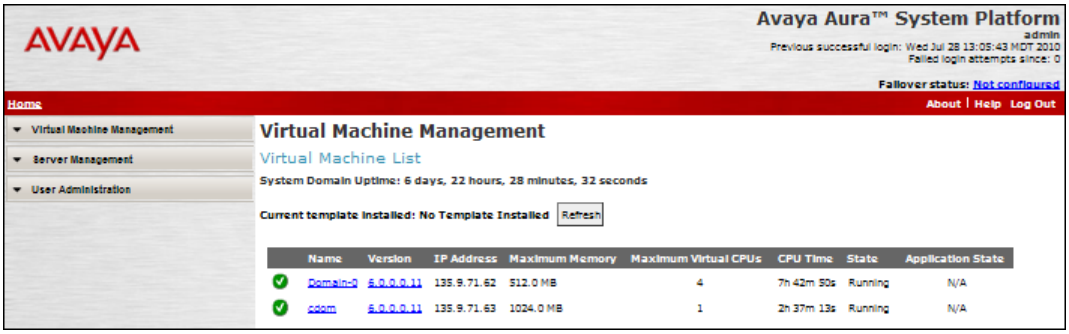
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix C on page 1679.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying Communication Manager operation

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading DEFINITY SI or R Server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the following existing DEFINITY Server to Communication Manager Release 6.2 on HP DL360 G7 Servers or Dell R610 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 6.2 on the new server.
- Installing translation file on Communication Manager Release 6.2.
- Administering IPSIs on Communication Manager Release 6.2.
- 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 6.2.

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: - HP DL360 G7 - Dell R610 • 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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

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

Before you begin

A cross-over cable to connect your services laptop directly to the processor.

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Procedure

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

Procedure

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 new servers

Installing 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 Dell R610 Server, see *Installing the Dell™ PowerEdge™ R610 Server*.
- For HP DL360 G7 Server, see *Installing the HP ProLiant DL360 G7 Server*.

Complete the procedures starting from “Installing System Platform and Communication Manager” through “Rebooting the server” on the first HP DL360 G7 Server or Dell R610 Server first. Repeat the procedures on the second HP DL360 G7 Server or Dell R610 Server.

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

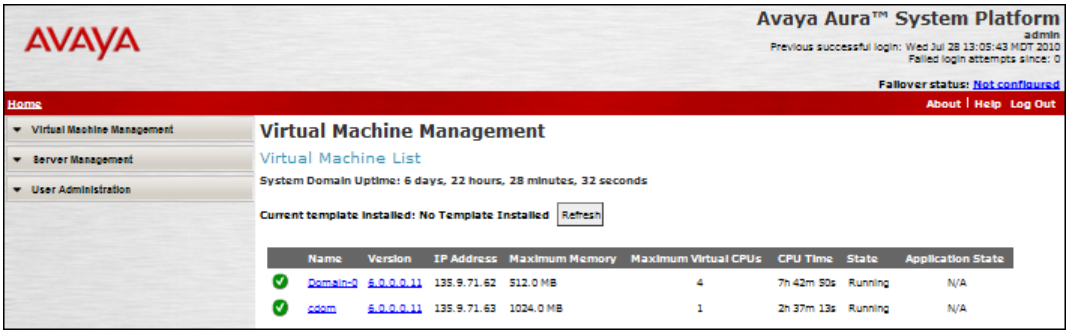
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Before you begin

Log on to System Management Interface.

About this task

You restore the translations only on the main server. When a 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server 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 status of restore process.

Result

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

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Appendix B on page 1667.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.
4. Click **Server Configuration** > **Duplication Parameters** and complete the configuration.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verification tasls on the HP DL360 G7 or Dell R610 Servers

Starting a SAT session

Before you begin

Log on to the services port from a directly connected laptop.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

Log on to System Management Interface of the standby server.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Log in as `craft` or `dadmin`.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Tasks on the first HP DL360 G7 or Dell R610 Server

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
3. On the Busy-Out/Release Server page, click **Release**.

Verifying the connection for server duplication

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. On the Ping page, in the **Endpoints to Ping** section, click **Other server via duplication link**.
4. Click **Execute Ping**.
   If the two endpoints are connected, the system displays the message `MessRecv`: 1.
5. In the navigation pane, click **Server** > **Status Summary** and perform the following:
   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

Before you begin

Install a Secure Shell (SSH) application such as PuTTY on your laptop.

Procedure

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. Select the **SSH** protocol.
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 host key of the server.

   The system displays the PuTTY window.
8. Log in as **craft** or **dadmin**.
9. Type `exit` and press `Enter` to close PuTTY.

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**

2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.
2. In the browser, choose one of the following options depending on server configuration:

   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

   - LAN access by host name

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

   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Administering the Communication Manager system parameters for IPSI

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.

6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the 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 pack

Before you begin

Start a SAT session.

About this task

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

About this task

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.

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

Before you begin

Start a SAT session.

About this task

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

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 in the **Circuit Packs Available for Synchronization** section.
5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for 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 all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display PASS in the **Results** field. If the **Results** field does not display PASS, troubleshoot the synchronization error.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

About this task

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

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 HP DL360 G7 Server or a Dell R610 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 load balance across the IPSIs throughout the port networks.

Decommissioning the PPN

About this task

Because you do not reuse the PPN on the upgraded system, you must relocate the port network circuit packs to the new media gateway.

Procedure

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

About this task

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

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 if you want 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 HP DL360 G7 or Dell R610 Server

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Verifying the Communication Manager operation

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.

3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Postupgrade tasks on the second HP DL360 G7 or Dell R610 Server

Connecting the server to network

About this task

At this point, the service outage occurs.

Procedure

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

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. To verify the connectivity to all IPSIs, in the **Query Type** section, select Query All and click **View**.

Releasing the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Busy-Out/Release Server**.

3. On the Busy-Out/Release Server page, click **Release**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the status for all operations is `UP STANDBY`.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Interchanging the servers

Before you begin

Log on to System Management Interface.

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Interchange Servers**.
3. Click **Interchange**.
   The system changes the roles of the active and standby servers.

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2 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 a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring Communication Manager Release 6.2 on S8300D Server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.2.

- Decommissioning the cabinets.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license file for Communication Manager Release 6.2. 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.

✔	Task	Description
	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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

Preupgrade administration

Connecting to the processor

Before you begin

Cross-over cable.

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Procedure

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

Before you begin

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)

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

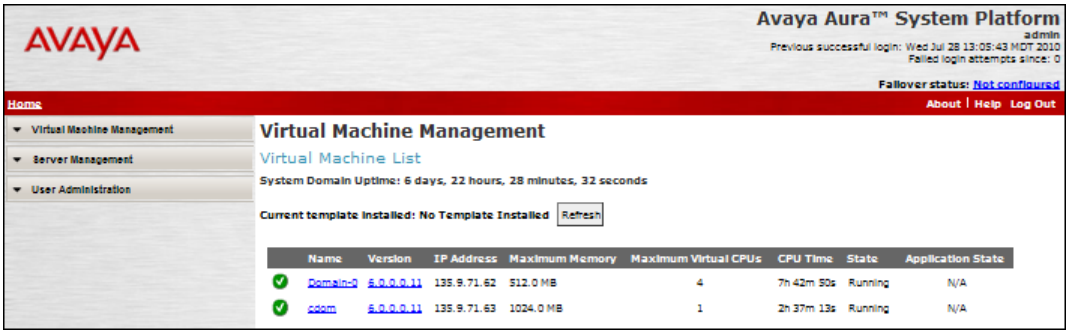
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

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

   Note:

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

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

Before you begin

Log on to System Management Interface.

About this task

You restore the translations only on the main server. When a 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server 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 status of restore process.

Result

When the restoration is complete, the system displays the following message:
`backup: 0: restore of <filepath/filepath> completed successfully.`

Configuring a branch gateway

About this task

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- Register the branch gateway with Communication Manager.
- Start a SAT session.

About this task

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:

- **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

The system displays a list of packages available for installation.

4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

Unplug the portable computer from the services port.

Removing fiber-related hardware

About this task

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

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

About this task

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

About this task

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

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 if you want 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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Verifying system status

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.

3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Perform the procedures related to Communication Manager Messaging only if Communication Manager Messaging is enabled on this server.

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.

4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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 6.2.1 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 on S8300D Server.
- Activating a preupgrade service pack on Communication Manager while on Release 4.0.5.
- Creating a data set with specific information that you back up and later restore on Communication Manager Release 6.2.1.
- 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.

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 6.2.1.

Checking the FTP, SFTP, or SCP server information

Before you begin

The customer server is accessible over the LAN for backups.

About this task

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

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

About this task

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

Procedure

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

To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.
    c. Enter `almsnmpconf` and record the output.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.

4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Before you begin

To use Telnet, enable the Telnet service for Communication Manager.

About this task

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

Procedure

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, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, 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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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, 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

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **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 FTP, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **Start Backup**.
6. Select the backup file from the list and click **Check Status**.

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

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

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`

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

   You can select four files at a time.
6. 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

Procedure

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

Procedure

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

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **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 FTP, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
5. Click **Start Backup**.
6. Select the backup file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

About this task

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 Appendix A on page 1661 to record the information.

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required

language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.

3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

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

Before you begin

CD/DVD for Communication Manager Release 4.0.5 or Release 5.2.1 as appropriate.

Procedure

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

Procedure

1. On the computer, 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 option 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

About this task

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

Procedure

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

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

   - LAN access by host name

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

   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. 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

Procedure

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

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing service pack

Before you begin

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

About this task

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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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**.
4. Click **Continue**.

Note:

Do not install the pre-upgrade service pack until instructed.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Configuring network parameters

Before you begin

- Obtain the host name, subnet mask, and IP addresses of the server and default gateway.
- Log on to System Management Interface.

About this task

You can configure the server data using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.

   The system displays the View/Restore Data Results page.
7. Select the backup file and click **Restore**.

8. To monitor the restore progress, select **Data Backup/ Restore** > **Restore History**.
   The system displays the Restore History page.
9. Select the backup file that you want to monitor and click **Check Status**.
   The system displays the Restore History Results page.
10. Click **Refresh** periodically until the message indicates that the restore is successful.
    This refresh process takes about 5 minutes.
11. Repeat Step 3 through Step 9 to restore:
    - The security dataset, if not performed in Step 7
    - The Communication Manager translations data
    - The messaging application data in the `audix-tr-name-msg` file
    - The messaging application announcements in the `audix-ann` file

Creating a super-user login

About this task

Note:

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

Procedure

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

Procedure

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

About this task

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 153.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server** > **Shutdown Server**.
3. Select the following check boxes:
   - **Restart server after shutdown**
   - **Shutdown even if this is the active server**
4. Click **Shutdown**.
   The system displays the `A server shutdown has been requested` message.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   The backup location must be a server on the customer LAN.
4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on the Maintenance Web page.

Procedure

1. In the navigation pane, click **Server** > **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 6.2.1) Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

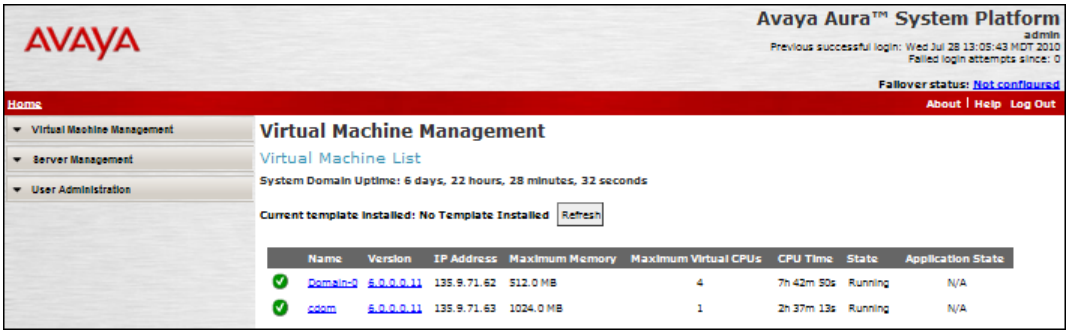
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.

4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   Important:

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:

- **Server Hardware**: okay
- **Processes**: okay

4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.

4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.

- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2.1 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 6.2.1.

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 6.2.1.

For S8300A Server, on Communication Manager release earlier than 5.2.1, perform the upgrade as instructed in the section “Upgrading the 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

Onsite preparation

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

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

worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Checking the FTP, SFTP, or SCP server information

Before you begin

The customer server is accessible over the LAN for backups.

About this task

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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 the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the devices from the server

Procedure

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the server

Before you begin

- 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.

About this task

⚠ 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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

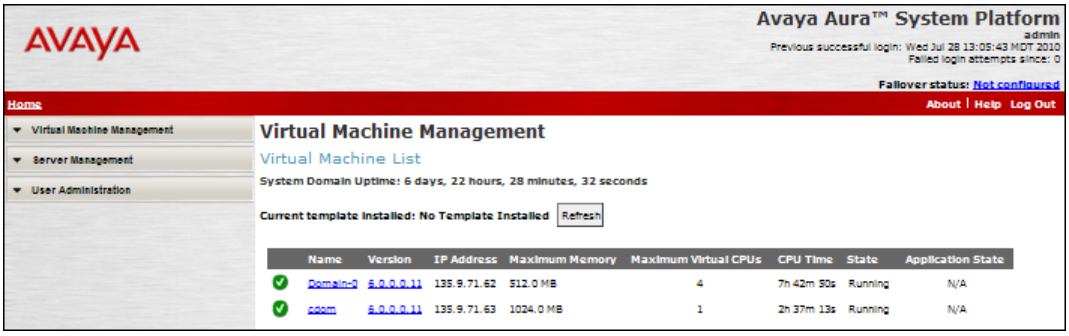
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.

4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   Important:

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.

6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.

4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

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

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2.1 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 6.2.1.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.
- Installing and configuring System Platform and Communication Manager Release 6.2 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.2.1.
- (Optional) Restoring Communication Manager Messaging data set.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.1.

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 6.2.1. 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 to perform 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

Before you begin

A CAT5 cross-over cable to connect your services laptop to the server.

Procedure

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

About this task

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

Procedure

1. Open a compatible Web browser.
2. If you log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying system status

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

Before you begin

To use Telnet, enable the Telnet service for Communication Manager.

About this task

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

Procedure

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, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, 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

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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.

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

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **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. In the **Backup Method** section, click **Network Device** and select a method from the list of 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Recording configuration information

About this task

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 Appendix A on page 1661 to record the information.

Procedure

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

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Before you begin

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)

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

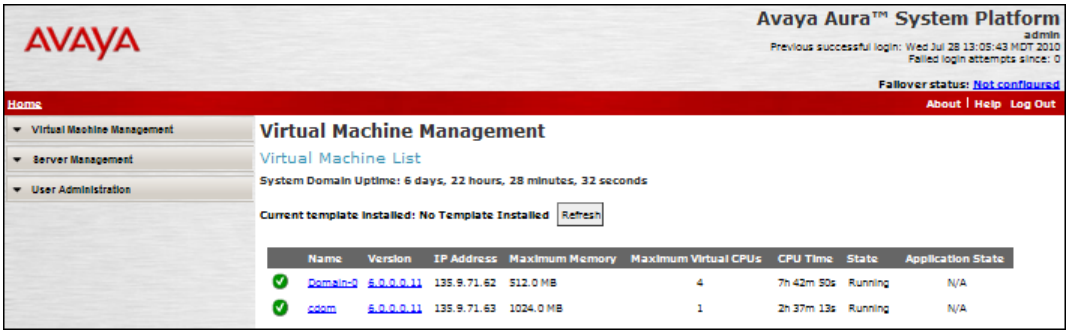
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory ***/vsp-template***:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

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

   Note:

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

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

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring a branch gateway

About this task

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- Register the branch gateway with Communication Manager.
- Start a SAT session.

About this task

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets.
See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.

3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Removing the G650 Media Gateway and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Turning off the power to the port network

Procedure

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 6.2.1 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 6.2.1.
- Installing a G430 or G450 Branch Gateway with an S8300D Server.

- Installing and configuring System Platform and Communication Manager Release 6.2 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.2.1.
- (Optional) Restoring Communication Manager Messaging data set.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.1.

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 6.2.1. 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	

✔	Task	Description
	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

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

Important:

Do not click **Submit**.

9. At 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 the product ID.

Clearing alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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

Procedure

1. Enter `status synchronization`.
2. Press `Enter` to verify that the clock synchronization is complete.
3. In the **Switching Capabilities** field, ensure the system displays `enabled`.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations (main only)

About this task

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

Procedure

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, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

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

    ⚠ Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Before you begin

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)

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

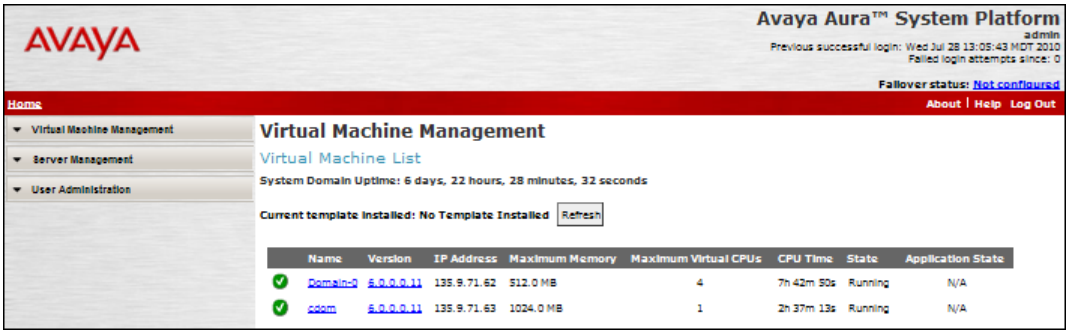
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory ***/vsp-template***:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

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

   Note:

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

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

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring a branch gateway

About this task

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- Register the branch gateway with Communication Manager.
- Start a SAT session.

About this task

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets.
See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.

7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Completion tasks on S8500 Server

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the server from the rack

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.

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

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.

4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.

- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Removing the G650 Media Gateway and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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 6.2.1 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.x.

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 6.2.1.

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 6.2.1.

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 6.2.1. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks on S8300 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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 the scheduled maintenance

Before you begin

Start a SAT session.

About this task

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

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

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

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

     The backup location must be a server on the customer LAN.
4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.

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

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.

4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Verify that you selected the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.

Disconnecting the devices from server

Procedure

Disconnect the USB CD/DVD reader from the server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote server.

- 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 you finish installing the Communication Manager template, do not configure Communication Manager and do not begin to administer the translations unless the procedures in this section instruct you.

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

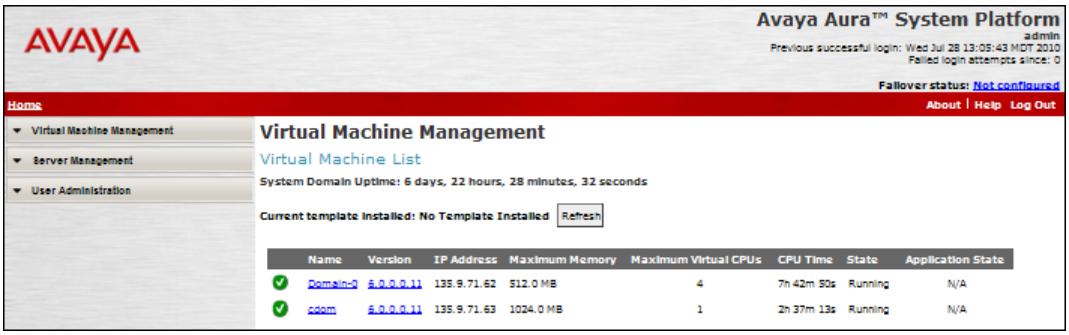
Note:

- You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack

- Solution template service packs
- Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.

3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

The system displays a list of packages available for installation.

4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.

2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
   You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.

3. Make test telephone calls to verify that the server is in operation after the upgrade.

Enabling scheduled maintenance

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Verifying the destination for scheduled backups

Before you begin

Log on to System Management Interface.

About this task

Communication Manager Release 6.x does not support creating a back up on a USB flash card.

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and perform one of the following:
   - To change the schedule backup, click **Change**.

     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

Before you begin

Log on to System Management Interface.

About this task

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

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Data Backup/Restore** > **Schedule Backup**.
3. Select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat Steps 2 and 3 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.

4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2 on S8300D Server running System Platform and the embedded survivable remote template (CM_SurvRemoteEmbed).

- 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 remote template.

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 6.2 on S8300D Server.
- Decommissioning the cabinets.
- Removing fiber connections and fiber hardware.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

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 6.2 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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

Preupgrade administration

Connecting to the processor

Before you begin

Cross-over cable.

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Procedure

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

Before you begin

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)

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

c. In the command line, type **ip_forwarding disable** and press **Enter**.

An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

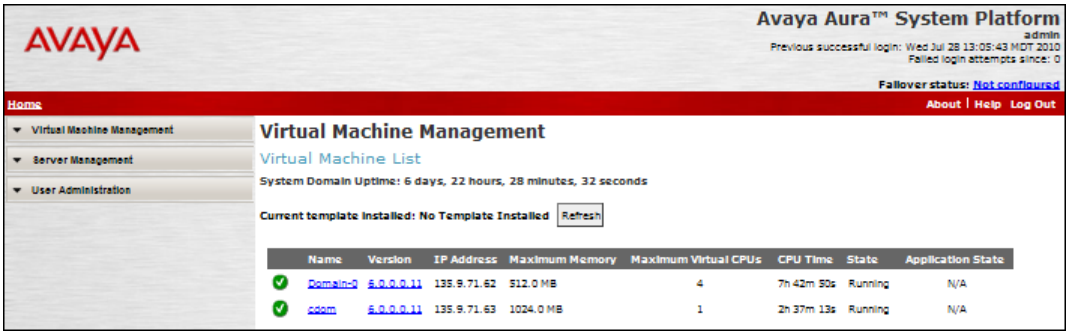
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.

5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- Register the branch gateway with Communication Manager.
- Start a SAT session.

About this task

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

About this task

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

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

About this task

Because you do not reuse any of the hardware in the cabinet on the upgraded system, you discard the cabinet.

Procedure

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 if you want 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

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the cabinet and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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 6.2.1 on an S8300D Server.

In this procedure, you 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 6.2.1.
- 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 6.2.1 configured as survivable remote server.

Prerequisites

USB DVD/CD-ROM drives

To upgrade S8300 Server to S8300D Server, you must install System Platform and Communication Manager 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 LED turns red and the system displays 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 FTP, SFTP, or SCP server information

Before you begin

The customer server is accessible over the LAN for backups.

About this task

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

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 S8300A Server

Clearing the ARP cache on the laptop computer

About this task

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 portable computer. If you fail to clear the cache, the computer does not connect to the server.

Procedure

1. To open the Run dialog box, click **Start** > **Run**
2. At the MS-DOS prompt, 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 prompt displays when the cache clears.
   - Displays the message `The specified entry was not found` when the specified IP address does not currently appear in the ARP cache.
4. Enter `exit`.

Accessing Maintenance Web Interface

Procedure

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

Procedure

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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Appendix on page 1661 of this book.

Procedure

1. On the **Server Configuration** menu, click **Configure Server**.

2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.

      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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. Click **Cancel**.

   Important:

   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 the product ID.
c. Enter `almsnmpconf` and record the output.

Recording configuration information

About this task

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 Appendix A on page 1661 to record the information.

Procedure

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

Before you begin

Log on to System Management Interface.

About this task

Record the backup scheduled for the existing server. You must submit the scheduled backups after the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.

3. On the Schedule Backup page, note the details of any backup schedules.

   You 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, 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

Before you begin

Log on to System Management Interface.

Procedure

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

   If the backup file size is large, there may be more than one `.tar` file.
5. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
6. Fill in the following fields:
   - **User Name**
   - **Password**

- **Host Name** which is the host IP address
- **Directory**

7. Click **Start Backup**.
8. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
9. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on the Maintenance Web page.

Procedure

1. In the navigation pane, click **Server** > **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

Procedure

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the S8300A Server

Before you begin

- Shut down the server.
- Ensure that **OK to Remove** LED on the server faceplate is steady.

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

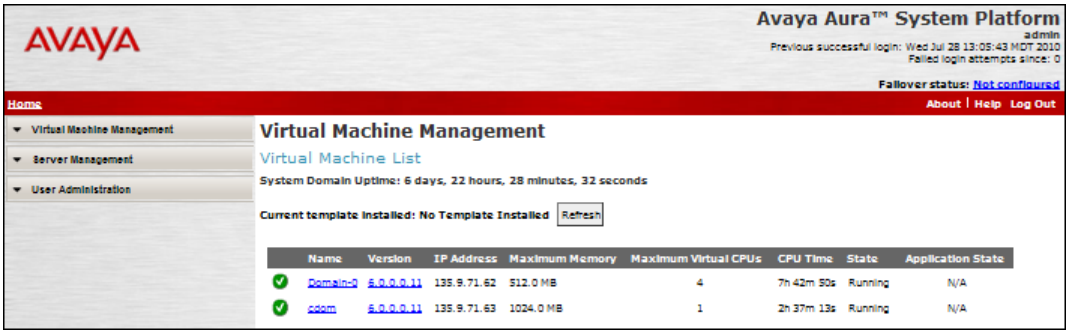
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory ***/vsp-template***:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

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

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring the alarming information

Before you begin

Log on to System Management Interface.

About this task

Configure the information provided in the worksheet available in Appendix A on page 1661.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter a `lmsnmpconf` 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

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Submitting the scheduled backups

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2.1 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 (CM_SurvRemoteEmbed).

The embedded survivable remote template supports 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 6.2.1.

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 6.2.1.

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 6.2.1.
3. Perform the upgrade to Release 6.2.1 as described in this section.

Onsite preparation

Accessing the System Management Interface

About this task

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

Procedure

1. Open a compatible Web browser.
2. In the browser, choose one of the following options depending on server configuration:

- LAN access by IP address

  To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.

- LAN access by host name

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

- Portable computer access by IP address

  To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.

3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:

a. Right-click and select **Paste**.

   The application copies the configuration information for the page.

b. On the **File** menu, click **Save As**.

c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Checking the FTP, SFTP, or SCP server information

Before you begin

The customer server is accessible over the LAN for backups.

About this task

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.

- To log in from a portable computer 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

Before you begin

Start a SAT session.

Procedure

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

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

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

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the devices from the server

Procedure

1. Disconnect the USB connected MODEM from the server.
2. Disconnect the USB CD/DVD reader from the server.

Replacing the server

Before you begin

- 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.

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

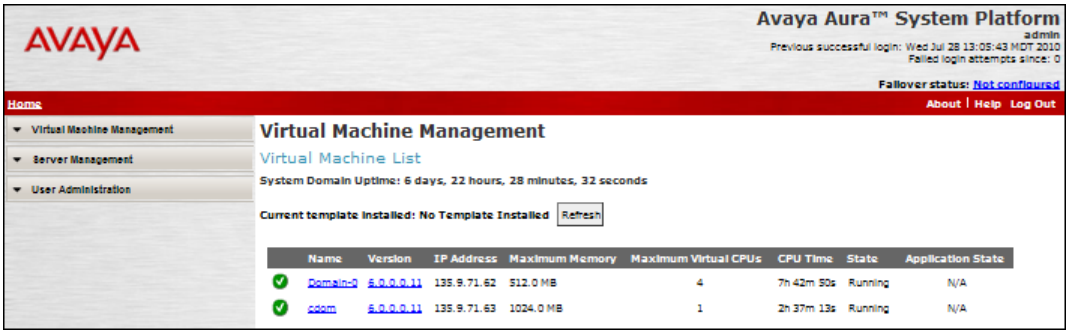
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.

6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring the alarming information

Before you begin

Log on to System Management Interface.

About this task

Configure the information provided in the worksheet available in Appendix A on page 1661.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter a `lmsnmpconf` 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

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.

8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Submitting the scheduled backups

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.
3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you 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 6.2.1 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 6.2 on the new server.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

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 6.2.1.

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 6.2.1. 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	

✔	Task	Description
	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

Before you begin

A CAT5 cross-over cable to connect your services laptop to the server.

Procedure

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

About this task

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

Procedure

1. Open a compatible Web browser.
2. If you log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying system status

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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.

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

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **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. In the **Backup Method** section, click **Network Device** and select a method from the list of 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 file from the list and click **Check Status**.

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

   ⚠ Caution:

   Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Before you begin

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)

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

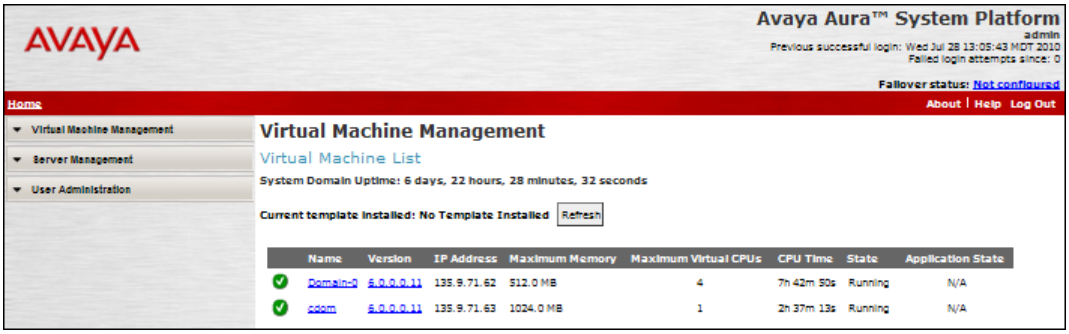
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- Register the branch gateway with Communication Manager.
- Start a SAT session.

About this task

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Removing the G650 Media Gateway and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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

Procedure

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 portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Turning off the power to the port network

Procedure

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 6.2.1 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 6.2 on the new server.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

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 6.2.1.

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 6.2.1. 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.

✔	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 on the S8500 Server

Upgrading branch gateways and survivable servers

About this task

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 you want to upgrade is the main server of 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:

Procedure

1. The branch gateway firmware
2. The media modules firmware
3. Communication Manager on a survivable remote server
4. Communication Manager on a survivable core server
5. Communication Manager on a main server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

iv. In the **Download size** field, enter the size of the backup `.tar` file.

If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Upgrade tasks on the S8300D Server

Inserting the S8300D Server in the branch gateway

Before you begin

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)

About this task

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.

Procedure

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

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

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

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
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:

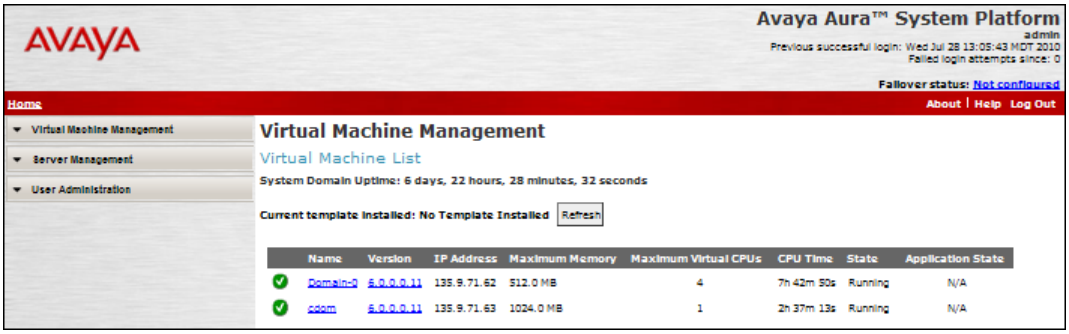
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.

- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.

3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

Use this procedure to configure a branch gateway to work with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

- Register the branch gateway with Communication Manager.
- Start a SAT session.

About this task

Use this procedure to administer a branch gateway with Communication Manager using the information provided in the worksheets available in Appendix A on page 1661.

Procedure

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

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Postupgrade tasks on S8300D Server

Verifying the Communication Manager operation

Accessing the System Management Interface

About this task

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

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

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

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

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

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

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

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you used.

Removing the G650 Media Gateway and the circuit packs

About this task

Discard any hardware you replaced during the upgrade.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Removing the server from the rack

Procedure

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 6.2.1 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.x.

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 6.2.1.

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 6.2.1.

For S8300D servers on releases of Communication Manager earlier than 5.2.1, upgrade to Release 5.2.1 before you upgrade them to Release 6.2.1. For more information, see *Upgrading Avaya Aura™ Communication Manager on Avaya S8xxx Servers* (03-602885).

Preupgrade tasks on S8300 Server

Accessing the System Management Interface

About this task

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

Procedure

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

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

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

To log in to the services port from a directly connected laptop, enter `192.11.13.6`.

3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Copying configuration information

You must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.
8. Click **Cancel**.

   Important:

   Do not click **Submit**.
9. At 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 the product ID.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.
   The system displays the Software Version page.
3. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, 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)**

  iii. In the **Communication Manager Messaging (CMM)** section, select **Translations, Names, and Messages**.

  iv. In the **Download size** field, enter the size of the backup `.tar` file.

  If the backup file size is large, there may be more than one `.tar` file.

4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:

   - **User Name**
   - **Password**
   - **Host Name** which is the host IP address
   - **Directory**

   When the backup process is complete, the system saves the `migration-60*.tar.gz` file to the location you specify in the **Directory** field. You must move the file to the services portable computer 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 file from the list and click **Check Status**.

When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:

- **User Name**
- **Password**
- **Host Name**
- **Directory**

  The backup location must be a server on the customer LAN.

4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.

4. Verify that you selected the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.

Disconnecting the devices from server

Procedure

Disconnect the USB CD/DVD reader from the server.

Upgrade tasks on the S8300D Server

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- System Platform
- The Communication Manager license

Note:

Do not install the Communication Manager license file when you upgrade a survivable remote 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   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 administrator.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

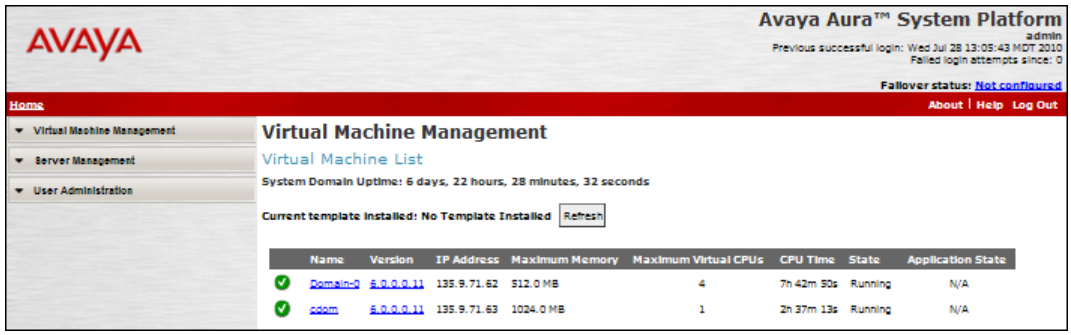
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Restoring the upgrade dataset

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

Note:

You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Configuring the alarming information

Before you begin

Log on to System Management Interface.

About this task

Configure the information provided in the worksheet available in Appendix A on page 1661.

Procedure

1. Configure the following alarm information:
   - **Alarms** > **SNMP Agents**
   - **Alarms** > **SNMP Traps**
2. At the command prompt, enter a `lmsnmpconf` 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

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

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

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

To install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Submitting the scheduled backups

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Schedule Backup**.

3. On the Schedule Backup page, select the scheduled backup and click **Change**.
4. On the Change Current Schedule page, click **Change Schedule**.
5. Repeat steps 3 and 4 for all the scheduled backups.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Logging off all administration applications

About this task

When you complete all the administration activities, log off from all the applications you 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 HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the existing DEFINITY Server CSI in a CMC to Communication Manager Release 6.2.1 on an HP DL360 G7 Server or Dell R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.2.1. You reuse the cabinet in the new system.

In this procedure, you replace the DEFINITY Server CSI with an HP DL360 G7 Server or Dell 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 6.2 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Installing translation file on Communication Manager Release 6.2.
- Administering IPSIs on Communication Manager Release 6.2.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.1. 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: - HP DL360 G7 - Dell R610 • 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 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. 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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

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

Before you begin

Cross-over cable.

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Procedure

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

Procedure

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, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

- Dell R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   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 administrator.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

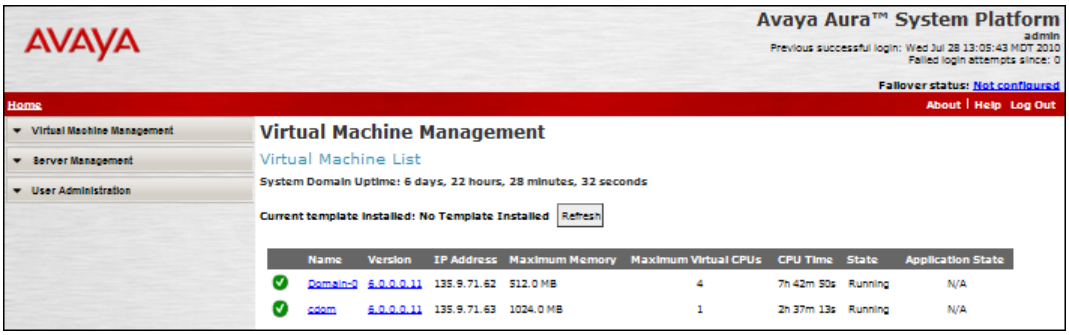
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

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

Before you begin

Log on to System Management Interface.

About this task

You restore the translations only on the main server. When a 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server 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 status of restore process.

Result

When the restoration is complete, the system displays the following message:
`backup: 0: restore of <filepath/filepath> completed successfully.`

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.

2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the 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 pack

Before you begin

Start a SAT session.

About this task

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

Unplug the portable computer from the services port.

Postupgrade tasks on HP DL360 G7 or Dell R610 Server

Testing the system using SAT commands

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

To install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.

5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading DEFINITY ONE/S8100 in CMC to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the existing S8100 Server in a CMC to Communication Manager Release 6.2.1 on an HP DL360 G7 Server or Dell R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.2.1. 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 HP DL360 G7 Server or Dell 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 6.2 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Installing translation file on Communication Manager Release 6.2.
- Administering IPSIs on Communication Manager Release 6.2.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.1. 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: - HP DL360 G7 - Dell R610 • 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 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. 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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

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

Before you begin

A cross-over cable to connect your services laptop directly to the processor.

Procedure

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

About this task

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.

Procedure

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

Procedure

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

Procedure

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

Before you begin

Start a Telnet session to access the processor circuit pack that is connected to the service laptop.

About this task

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.

Procedure

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, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

- Dell R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.

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 administrator.
   c. In the command line, type **ip_forwarding disable** and press **Enter**.

      An alternative to the above command is **service_port_access disable**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

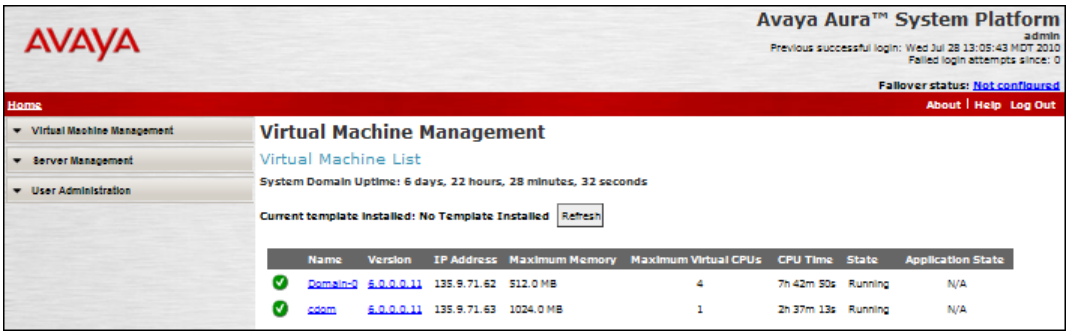
3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.

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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**

- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
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

Before you begin

Log on to System Management Interface.

About this task

You restore the translations only on the main server. When a 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server 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 status of restore process.

Result

When the restoration is complete, the system displays the following message:

```
backup: 0: restore of <filepath/filepath> completed successfully.
```

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 HP DL360 G7 or Dell R610 Server

Testing the system using SAT commands

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

To install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.

2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.

2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading Avaya IP600/S8100 Server in G600 to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the existing S8100 Server in G600 Media Gateway to Communication Manager Release 6.2.1 on a HP DL360 G7 Server or Dell R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.2.1. 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 HP DL360 G7 Server or Dell 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 6.2 on the new server.
- Installing Communication Manager Messaging (optional).
- Installing translation file on Communication Manager Release 6.2.

- (Optional) Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.2.
- Adding circuit packs to the media gateway.
- Decommissioning PPNs.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.1.

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: - HP DL360 G7	

✔	Task	Description
	- Dell R610 • 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 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. 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

Before you begin

Start a SAT session.

About this task

Perform this procedure to safeguard the system, in case you need to bring the system to its current configuration.

Procedure

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 the filesync errors, if any.

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

Before you begin

A cross-over cable to connect your services laptop directly to the processor.

Procedure

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

About this task

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.

Procedure

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

Procedure

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

Procedure

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

Before you begin

Start a Telnet session to access the processor circuit pack that is connected to the service laptop.

About this task

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.

Procedure

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, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

- Dell R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   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 administrator.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

   An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

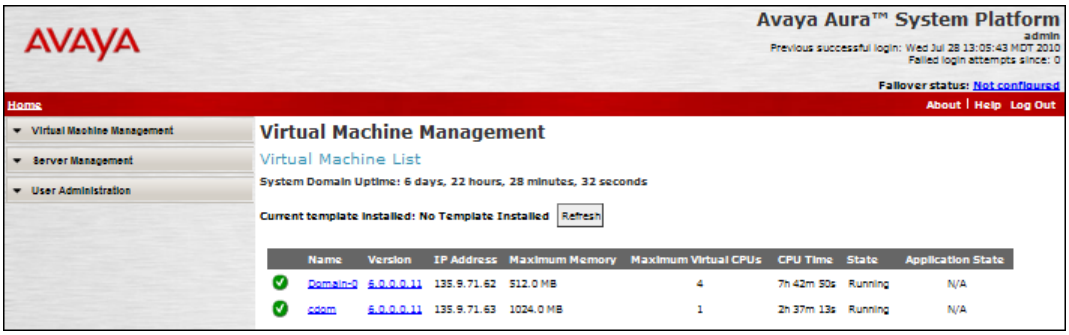
Note:

- You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
- This is a secure site. If you get a certificate error message, follow the instructions on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack

- Solution template service packs
- Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

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

Before you begin

Log on to System Management Interface.

About this task

You restore the translations only on the main server. When a 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.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server 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 status of restore process.

Result

When the restoration is complete, the system displays the following message:
`backup: 0: restore of <filepath/filepath> completed successfully.`

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

Important:

The Communication Manager Messaging processes stop during RFU installation.

If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.

2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
   You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Procedure

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

Before you begin

Turn off power to the carrier or the media gateway.

⚠ Caution:

Failure to turn off the power can result in electric shock.

About this task

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.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 HP DL360 G7 or Dell R610 Server

Testing the system using SAT commands

Procedure

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

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

To install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.
   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms you want to clear.
4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session. For information, see:
   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431
   - *Avaya Aura™ Communication Manager Server Alarms*, 03-602798

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Registering the system

Use the standard procedure to register the system.

Upgrading S8300 Server to the HP DL360 G7 or Dell R610 Server

Introduction

This section describes the procedure to upgrade the embedded S8300 Server in G430 or G450 Branch Gateway to Communication Manager Release 6.2.1 on an HP DL360 G7 Server or Dell 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 6.2.1.
- You install the standalone HP DL360 G7 Server or Dell 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 6.2.1.
- Installing and configuring System Platform and Communication Manager Release 6.2 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.2.
- (Optional) Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.2.
- Installing G650 Media Gateway.
- Adding circuit packs to the media gateway.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.1.

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 6.2.1. 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 HP DL360 G7 Server or Dell R610 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 you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the following software: • System Platform • the required Communication Manager template	
	Obtain the required hardware: • One of the following servers, as appropriate: - HP DL360 G7 - Dell R610 • Circuit packs: - TN2312BP IPSI - TN799DP C-LAN	
	Ensure that the circuit packs are on the latest firmware.	For information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the

✔	Task	Description
		Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks on the S8300 Server

Accessing the System Management Interface

About this task

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. In the browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate local area network, enter the unique IP address of Communication Manager in the standard dotted-decimal notation.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying the current software release

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Software Version**.

   The system displays the Software Version page.
3. 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 must record the configuration information available on System Management Interface of the existing release of Communication Manager. You use this information 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

Before you begin

- Log on to System Management Interface.
- Create a folder on your computer to store the configuration files. You can easily find files stored in a new folder.
- Decide the application, for example, Microsoft Word, Wordpad, or Microsoft Paint, to which you want to copy the configuration information.

About this task

The system backs up most of the server data and restores the data after the upgrade is complete. However, you must record some of the server data manually in the appropriate worksheet provided in the Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661 of this book.

Procedure

1. On the **Installation** menu, click **Configure Server**.
2. On the Configure Server page, 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 on which you want to copy the configuration information, for example, Microsoft Word, Wordpad, or Microsoft Paint, and perform the following:
   a. Right-click and select **Paste**.
      The application copies the configuration information for the page.
   b. On the **File** menu, click **Save As**.
   c. Select a folder that you created on your computer to store the configuration files. 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 must reinstall these files after the upgrade.

8. Click **Cancel**.

   Important:

   Do not click **Submit**.

9. At 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 the product ID.

Checking the FTP, SFTP, or SCP server information

Before you begin

The customer server is accessible over the LAN for backups.

About this task

Before you begin the upgrade, you need to back up the system data to an FTP, SFTP, or SCP server over the customer LAN. For Communication Manager Release 1.x, 2.0 or 2.0.1, the system supports only FTP.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. Perform one of the following:
   - To log 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`.
   - To log in from a portable computer 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

Procedure

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 the scheduled maintenance

Before you begin

Start a SAT session.

About this task

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you must reschedule the daily maintenance activity.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Communication Manager backup

Perform this routine backup before you perform any maintenance activity.

This backup is not specifically related to the upgrade. However, perform the routine backup for safeguarding the system, in case you need to return 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. However, Releases 1.x, 2.0 and 2.0.1 only support backup to an FTP server.
- A flashcard using the USB-connected external compact flash drive. However, Release 6.x, does not support the use of flashcard to restore files to System Platform.

Backing up files to another server

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
2. In the **Data Sets** section, select **Full Backup**.
   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.
   If the size of the backup file is large, you may have more than one `.tar` file.
4. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
5. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Copying files to the server

Before you begin

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.

   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.
4. Click **Continue**.

Next steps

Important:

If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:

- **User Name**
- **Password**
- **Host Name**
- **Directory**

  The backup location must be a server on the customer LAN.

4. Click **Submit**.
   The system displays the Linux Migration - Backup Results dialog box.
5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    ⚠ Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.

3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Upgrade tasks on HP DL360 G7 or Dell R610 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

- Dell R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   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 administrator.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

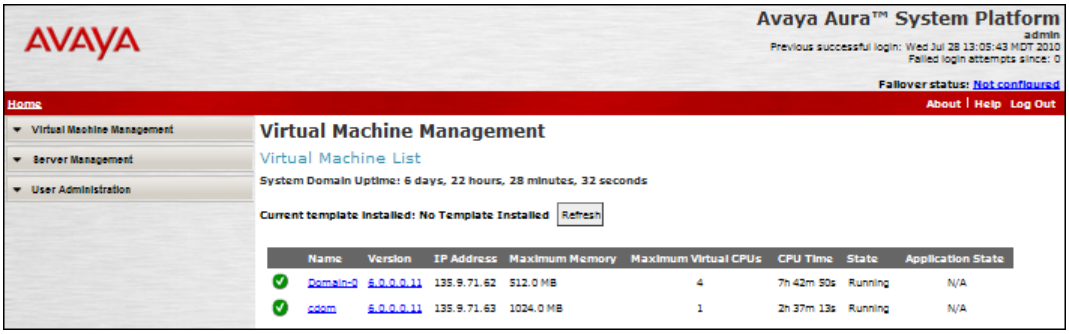
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.

2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.

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

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.

- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.

4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.

2. In **Frequency** section, select **Display Once**.
3. Click **View**.
   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   Important:

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server.`

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system displays a list of packages available for installation.
4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.
2. Enter `busyout signaling-group` <*num*>, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group` <*num*>. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
      You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.

b. On the **Administration** menu, click **Server (Maintenance)**.
c. Click **Server** > **Process Status**.

Shutting down the S8300 Server

Shutting down the server

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Turning off the power to the control cabinet

Procedure

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. 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

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.

3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 the HP DL360 G7 or Dell R610 Server

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.

2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

To install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.

3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Note:

Contact Avaya Support at http://support.avaya.com if:

- You need to repeatedly terminate a backup operation manually.
- System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.
4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Upgrading S8400 Server to the HP DL360 G7 or Dell R610 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 6.2 on an HP DL360 G7 Server or Dell R610 Server.

In this upgrade scenario, the existing system, with modifications, becomes a port network in the new system running Communication Manager Release 6.2.1. 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 HP DL360 G7 Server or Dell 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 6.2.1.

- Installing and configuring System Platform and Communication Manager Release 6.2 on the new server.
- (Optional) Installing Communication Manager Messaging.
- Restoring the data set on Communication Manager Release 6.2.
- (Optional) Restoring Communication Manager Messaging data set.
- Administering IPSIs on Communication Manager Release 6.2.
- Adding circuit packs to the media gateway.
- Completing the postupgrade administration tasks on Communication Manager Release 6.2.

You require a new license for Communication Manager Release 6.2.

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 6.2. 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
	Ensure that you redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.
	Verify that you have the following software: • System Platform • the required Communication Manager template	_
	Obtain one of the following servers, as appropriate: • HP DL360 G7 • Dell R610	_
	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* on the Avaya Support Web site at http://support.avaya.com.

Documentation checklist

To complete the system upgrade, obtain *Installing and Configuring Avaya Aura™ Communication Manager* (03-603558) from the Avaya Support Web site at http://support.avaya.com. This document provides the instructions for installing and configuring Communication Manager.

Preupgrade tasks on the S8400 Server

Connecting to the server

Before you begin

A CAT5 cross-over cable to connect your services laptop to the server.

Procedure

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

About this task

The System Management Interface (SMI) was formerly known as Maintenance Web Interface.

Procedure

1. Open a compatible Web browser.
2. If you log in to the services port from a directly connected laptop, enter `192.11.13.6`.
3. Press `Enter`.

   If the browser does not have a valid security certificate, the system displays 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 gain access to this server or other S8xxx servers again, click Install **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 home page of the Communication Manager SMI.

Verifying system status

Before you begin

Start a SAT session.

About this task

Verify the groups that are in-service and the groups that 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.

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Alarms** > **Current Alarms**.
3. In the **Server Alarms** section, select the alarms you want to clear and click **Clear** or **Clear All**.
4. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Enabling the Telnet service

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Security** > **Server Access**.
3. Click **Enable** for the following services:
   - **Telnet Server (23)**
   - **SAT (Telnet 5023)**
4. Click **Submit**.

Starting a SAT session

Before you begin

To use Telnet, enable the Telnet service for Communication Manager.

About this task

If the Telnet service is disabled, use SSH to gain access to SAT.

Procedure

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, using Telnet, enter `telnet 192.152.254.201 5023`.
   - If you are logging to the server using a laptop that is directly connected to the services port, 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

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Disabling the scheduled maintenance

Before you begin

Start a SAT session.

About this task

The scheduled daily maintenance may interfere with the server upgrade. To prevent this, you must reschedule the daily maintenance activity.

Procedure

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.

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

Procedure

1. In the navigation pane, click **Data Backup/Restore** > **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. In the **Backup Method** section, click **Network Device** and select a method from the list of 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 file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Recording configuration information

About this task

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 Appendix A on page 1661 to record the information.

Procedure

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

Before you begin

- Obtain the latest service pack files from the Avaya Support Web site at http://support.avaya.com.
- Log on to System Management Interface.

About this task

To copy the preupgrade service pack or service pack to the server:

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Miscellaneous** > **Download Files**.
3. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
4. Click **Browse** to open the **Choose File** window on your computer.
5. Select the files that you need to copy to the server and click **Open**.
   You can select four files at a time.
6. Click **Download** to copy the files to the server.
   The system copies the files to the default file location.

Installing the preupgrade service pack

Before you begin

Log on to System Management Interface.

About this task

To prepare the system for an upgrade to Communication Manager Release 6.2, install the preupgrade service pack as appropriate for Release 5.2.1 or Release 4.0.5.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server Upgrades** > **Manage Updates**.
3. 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 `... 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**.

4. Click **Continue**.

Next steps

Important:
If you require to rollback the upgrade, you must deactivate the preupgrade patch.

Backing up Communication Manager

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure to generate a backup file that you later restore on the Release 6.2.1 system during the upgrade.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.2**.
3. On the Linux Migration to CM 6.2 - Backup Initiate page, complete the following fields:
    - **User Name**
    - **Password**
    - **Host Name**
    - **Directory**

    The backup location must be a server on the customer LAN.
4. Click **Submit**.
    The system displays the Linux Migration - Backup Results dialog box.

5. Click **Status** to view the backup history.
   The system displays the Backup History page and a list of recent backups.
6. Select the backup file from the list and click **Check Status**.
   When the backup is complete, the system displays the message `Backup successful`.

⚠ Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Checking for backed up files

Procedure

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 Communication Manager Messaging is enabled on this system, obtain the required language packages, if you have not already obtained the packages before arriving at the site, leave a test message and shut down Communication Manager Messaging before you back up the custom announcement sets.

Custom announcement sets are announcement sets that customer creates. Back up the custom announcement sets. You restore the announcement sets after the upgrade. For more information on announcement sets, see the documentation for Communication Manager Messaging.

About language packages and announcement sets

Communication Manager Messaging offers standard announcement sets in several languages. All Communication Manager Messaging systems include the following announcement sets.

- Standard American English
- Terse American English
- Telecommunication Device for the Deaf (TDD)

You can download the standard announcement sets in other languages from the Avaya Support Web site at http://support.avaya.com. The announcement sets for a specific language are delivered in an `.rpm` file called a *language package*. After you download the required language packages, write the language packages to a CD-ROM. You install the language packages later on the upgraded system.

Identifying the language packages

Before you begin

Log on to System Management Interface.

About this task

If a language package is installed on the existing system, the same language package must be installed after an upgrade and before you restore the messaging translations. If you do not install the language package before you restore the messaging translations, Communication Manager Messaging fails to start. For example, if British English is installed on the existing system, install British English on the upgraded system before you restore the messaging translations.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **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 must download the additional language packages from a language CD. After the upgrade, install the language packages on Communication Manager.

Backing up custom announcement sets

Before you begin

Log on to System Management Interface.

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Messaging Administration** > **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 the language packages on page 48.
3. On the **Administration** menu, click **Server (Maintenance)**.
4. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
5. In the **Data Sets** section, select **Specify Data Sets**.
6. Select the **Communication Manager Messaging (CMM)** check box and click **Announcements**.
7. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
8. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.
    When the backup is complete, the system displays the message `Backup successful`.

Caution:

Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Setting up the test data

Procedure

1. Create a test station and a corresponding subscriber mailbox.
2. Call the messaging hunt group and log in 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

Procedure

1. Perform one of the following:
   - For Communication Manager earlier than Release 5.2.1, on Maintenance Web Interface, click **Miscellaneous** > **Messaging Administration**.
   - For Communication Manager Release 5.2.1 or later, on System Management Interface, click **Administration** > **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. The shutdown process takes a few minutes to complete. After messaging stops, the Web page displays the status information.

Backing up Communication Manager Messaging

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
3. In the **Data Sets** section, select **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 back up `.tar` file.

   If the backup size is large when you install embedded applications, such as Communication Manager Messaging, there may be more than one `.tar` file.
6. In the **Backup Method** section, click **Network Device** and select a method from the list of options.
7. Fill in the following fields:
   - **User Name**
   - **Password**
   - **Host Name** which is 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 file from the list and click **Check Status**.

    When the backup is complete, the system displays the message `Backup successful`.

    Caution:

    Check the text to verify that there are no error messages. If you ignore the error message, the back up of the files fails.

Upgrade tasks on HP DL360 G7 or Dell R610 Server

New server

Complete the upgrade procedures described in the following sections on the new server. At this point, you turn on the new server but you do not connect to the network.

The new server can be one of the following:

- HP DL360 G7 Server

  For instructions to install, see *Installing the HP ProLiant DL360 G7 Server.*

- Dell R610 Server

  For instructions to install, see *Installing the Dell™ PowerEdge™ R610 Server*.

Installing System Platform and Communication Manager

Install System Platform, latest service pack for System Platform, and the Communication Manager template on the server. For information on the service pack for System Platform, see the release notes for Communication Manager available at http://support.avaya.com.

For instructions to install, see *Implementing Avaya Aura® Communication Manager*, 03-603558:

- 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

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:

a. Start an SSH session.
b. Log in to System Domain (Domain-0) as administrator.
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 administrator.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

      An alternative to the above command is **`service_port_access disable`**.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console 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 39.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

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.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

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:

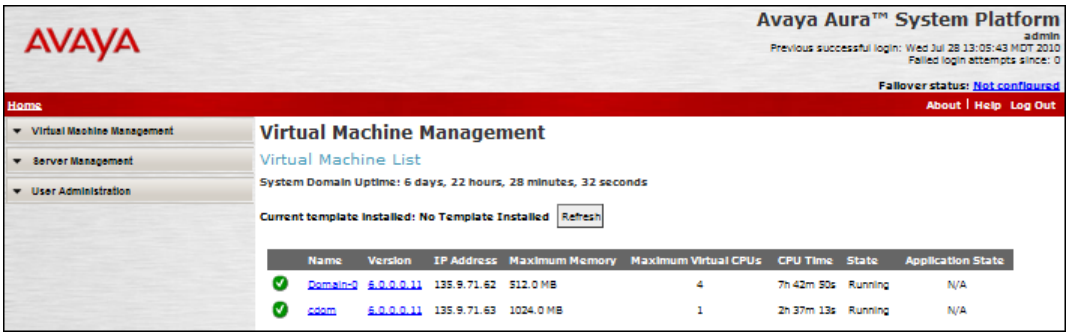
   - You can connect using `http`, but you will be immediately redirected to `https`. **Https** is the only method for accessing Web Console administration pages.
   - This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on 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.



Verifying the software version

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. Verify the version of the software and the template installed on the system.

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
   - **Avaya Downloads (PLDS)**
   - **HTTP**

- **SP Server**
- **SP CD/DVD**
- **SP USB Disk**
- **Local File System**

4. If you selected **HTTP**, enter the patch URL.
   Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
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

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires. (See ”Downloading patches” or “Related Topics”.)
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  - System Platform service packs
  - System Platform feature pack
  - Solution template service packs
  - Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

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

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

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 the 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 is 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 the Logon page generates. 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 home page of the Communication Manager System Management Interface.

Copying files to the server

Procedure

1. In the navigation pane, click **Miscellaneous** > **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.

   Note:

   Do not select the **Install this file on the local server** check box.
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

Before you begin

- Log on to System Management Interface.
- Ensure that the license file is valid.

  Note:

  You do not need a license file to upgrade a survivable core server or a survivable remote server.
- Install the latest service pack for Communication Manager Release 6.2.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 **File 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 you did not connect the server to the network, you must select **Local Directory**.
4. Click **View**.
5. Select the files to restore. For example, `migration-60_*.tar.gz` here, `*` is `hostname_hhmmss_YYYYMMDD`.
6. Click **Restore**.

Configuring the server data

Before you begin

Log on to System Management Interface.

About this task

Configure the server data using the information provided in the worksheets in Worksheet for upgrading Communication Manager to simplex and embedded templates on page 1661.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Server Configuration** > **Server Role** and complete the configuration.
3. Click **Server Configuration** > **Network Configuration** and complete the configuration.

Starting Communication Manager Messaging

Before you begin

You must have a valid license for Communication Manager.

Log on to System Management Interface.

Procedure

1. Click **Server** > **Process Status**.
2. In **Frequency** section, select **Display Once**.
3. Click **View**.

   The system displays the status of the services running on the system.
4. Ensure that the system displays the UP status for Messaging. If not, start the messaging service:
   a. Click **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

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.

2. In the **Miscellaneous** field, click **Download Files**.
3. To download the remote field update (RFU), click the appropriate download method from the following:
   - **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. To download the remote field update (RFU), click the appropriate download method from 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

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.
   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   Important:

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Copying language packages to the server

Before you begin

- Obtain a CD-ROM that contains the language packages.
- Log on to System Management Interface.

About this task

Copy the language packages to the server only if:

- Communication Manager Messaging is enabled.
- You identify any language packages on the system. For instructions, see Identifying the language packages on page 48.

Procedure

1. Insert the language CD-ROM in the CD-ROM drive of your portable computer.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Miscellaneous** > **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-ROM and click **Open**.

   You can select four files at a time from the language CD-ROM that you want to copy to the server.
6. Click **Download**.
   The system copies the language files to the `/var/home/ftp/pub` directory.

   The transfer is complete when the system displays `Files have been successfully downloaded to the server`.

Installing language packages

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Messaging**.
2. In the navigation pane, click **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

The system displays a list of packages available for installation.

4. Select the language packages to install.
5. Click **Install selected packages**.

Restoring custom announcements

Before you begin

Log on to System Management Interface.

About this task

You can restore custom announcements only if you backed up custom announcement sets. See Backing up custom announcement sets on page 49.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **View/Restore Data**.
3. Select **Network Device**.
4. In the **Method** field, select `ftp`.
5. Enter the following FTP parameters:
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**
6. Click **View**.
   The system displays the View/Restore Data Results page.
7. Select the custom announcement set you want to restore. For example, `audix-announcement*.tar.gz`.
8. Click **Restore**.

Restoring Communication Manager Messaging data

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **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 backup file you want to restore. For example, `audix-tr-name-msg*.tar.gz`.
7. Click **Restore**.

Administering the signaling group for Communication Manager and Communication Manager Messaging

Before you begin

- Start a SAT session.
- 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 the `status link procr` command.

About this task

In Release 6.x, Communication Manager and Communication Manager Messaging share the same IP address. Therefore, you must change the administered signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

The following example demonstrates how to change the signaling group and node name to support communication between Communication Manager and Communication Manager Messaging.

Procedure

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 use temporarily.

2. Enter `busyout signaling-group <num>`, where <*num*> is the Messaging Signaling Group number. Typically the Messaging Signaling Group number is 99.
3. Enter `change signaling-group <num>`. Typically the <*num*> is 99:
   a. Record the value of the **Far-end Node Name** field.
   You change this node name in Step 4. Typically the data in this field is `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

Procedure

1. On the **Administration** menu, click **Messaging**.
2. Click **Switch Link Admin.** > **Signal Group 1**.
3. In the **Messaging TCP port** field, enter `11720`.

Rebooting the server

Before you begin

System Platform Web Console

Procedure

1. Click **Virtual Machine Management** > **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**. The reboot process takes about 1 minute. To confirm that the reboot is complete:
   a. Log on to System Management Interface.
   b. On the **Administration** menu, click **Server (Maintenance)**.
   c. Click **Server** > **Process Status**.

Upgrade tasks on the cabinet

Existing hardware upgrade

You must upgrade and administer the existing PN to prepare the existing system for upgrade. 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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Shutdown Server**.
3. Select **Delayed Shutdown**.
4. Clear the **Restart server after shutdown** check box.
5. Click **Shutdown**.
   The power-on LED blinks slowly.
6. Wait about 30 seconds before you perform the next step.

Disconnecting the portable computer from the server

Procedure

Disconnect the services portable computer from the server.

Postupgrade administration

Tasks performed on the new server

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

About this task

Administer the IPSI related system parameters on Communication Manager.

Procedure

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.
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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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

Procedure

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

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.

3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number ___**.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Verifying firmware version

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **IPSI Firmware Upgrades** > **IPSI Version**.
3. In the **Query Type** section, click **Query All**.
4. Click **View**.
5. 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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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 the HP DL360 G7 or Dell R610 Server

Verifying the Communication Manager operation

Performing an integrity check

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Server** > **Status Summary**.
3. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
4. In the navigation pane, click **Server** > **Process Status**.
5. In the **Frequency** section, click `Display Once`.
6. Click **View**.
7. Verify that the system displays `UP SIMPLEX` for all operations.
8. Use Telnet to connect to a device outside the server and ping the IP address of Communication Manager.

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use 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

Before you begin

Start a SAT session.

Procedure

1. Enter `newterm`.
2. If you see the `Warning: Translation corruption detected . . .` message, follow the escalation procedure for translation corruption before you continue with the next procedure.

Testing the system using SAT commands

Procedure

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

Procedure

1. Enter `list configuration all`.
2. Verify that the software is communicating with all media modules and that the reports list all media modules.
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

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

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 the filesync errors, if any.

Installing the phone message file

Before you begin

If the phone message file is installed on the existing system, identify the file.

Procedure

To install a phone message file, see *Administering Avaya Aura™ Communication Manager* (03-300509).

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. To examine the alarm log, in the navigation pane, click **Alarms** > **Current Alarms**.
3. If the system lists any alarms, click **Clear** or **Clear All**.
4. Resolve any new alarms that appear since the upgrade. For more information, see *Avaya Aura™ Communication Manager Server Alarms, 03-602798*.

Backing up configuration information

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup.

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.

Procedure

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.
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**.

   The backup progress window opens in the **Backup** tab, displaying backup event messages with corresponding timestamps. The window remains open until any of the following events occur:
   - The operation concludes successfully.
   - You manually terminate the operation.
   - A system error condition abruptly halts the operation.

   Note:

   Contact Avaya Support at http://support.avaya.com if:
   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors

Verifying the Communication Manager Messaging test data

Procedure

1. Call the messaging hunt group and log in to the test mailbox.
2. Verify that the system plays the test name.
3. Verify that the system plays the test message.

4. Call the test station and verify that the system plays the test greeting.
5. Remove the test station and the corresponding test mailbox.

Backing up Communication Manager Messaging data

Before you begin

Network server to back up data.

Procedure

1. Log in to the System Management Interface Web page.
2. Select **Specify Data Sets**.
3. Select the **Messaging** checkbox.
4. Select **Messaging 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

About this task

When you complete all the administration activities, log off from all the applications you used.

Registering the system

Use the standard procedure to register the system.

Appendix A: Worksheet for upgrading Communication Manager to simplex and embedded templates

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 a simplex survivable core template, simplex survivable remote template, embedded survivable core template, or embedded survivable remote template.

When you restore the upgrade dataset, on the Server Role Web page, the system automatically populates the following fields:

- **Server Role**
- **SID**
- **MID**
- **Memory Setting**
- **Media Gateway serial number**

In all the blank fields, enter the values manually using this worksheet.

Note:

IPv6 has restricted usage. Therefore, unless instructed otherwise, keep IPv6 disabled and do not enter 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**	-
Registration address IPv6		Does not exist in Release 5.2.1	-

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
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.x.

Network Configuration

When you restore the upgrade dataset, on the Network Configuration Web page, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values manually using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

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 configured **CM Hostname** on System Platform: • As an FQDN, the Web page automatically populates the **CM Hostname** field in Communication Manager. • As simple hostname, you can configure the **CM Hostname** 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 you configured **Domain Search list** on System Platform, the

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			system populates the **Domain Search list** field automatically in Communication Manager. If **Domain Search list** is not configured on System Platform, you can configure the **Domain 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 the System Platform Web Console at the time of installation.
Secondary DNS		**Configure Server > DNS**	Entered on the System Platform Web Console at the time of installation.
Tertiary DNS		**Configure Server > DNS**	System Platform supports only two DNS values. System Platform 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	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	View only. Populated during the installation of Communication Manager template.
eth0 functional assignment	PE assigned or PE unused	**Configure Server > Set Identities**	-

Appendix B: Worksheet for upgrading Communication Manager to duplex template

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.x server on a duplex main/survivable template.

When you restore the upgrade dataset, on the Server Role Web page, the system automatically populates the following fields:

- **Server role**
- **SID**
- **MID**
- **Memory Setting**

In all the blank fields, enter the values manually using this worksheet.

Note:

IPv6 has restricted usage. Therefore, unless instructed otherwise, keep IPv6 disabled and do not enter 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		The system populates after you restore the dataset. Also, see Help on Server Role Web page.

Network Configuration

Server 1

When you restore the upgrade dataset, on the Network Configuration Web page, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values manually using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**

- **DNS**

• System Platform Web Console, **Server Management** > **Network Configuration**.

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 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 you configured **Domain Search List** on System Platform, the system automatically populates **Domain Search List** field in

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			Communication Manager. If you did not configure **Search Domain list 1** 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. System Platform 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 **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	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

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			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 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.

Field	Value	Method for obtaining from CM Release 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	-

Network Configuration

Server 2

When you restore the upgrade dataset, on the Network Configuration Web page, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values manually using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

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**	-

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
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.x, **Domain Search List** is a single field and accepts comma separated values. Combine the values obtained from **Domain Search List** 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 you configured **Domain Search List** on System Platform, the system automatically populates the **Domain Search List** field in Communication Manager. If you did not configure **Search Domain list 1** 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**	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. System Platform does not automatically populate the third DNS value.
Server ID		**Status Summary > ID**	-
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.

Field	Value	Method for obtaining from CM Release 5.2.1	Note
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. 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
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: Worksheet for upgrading Communication Manager on simplex to duplex template

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 a duplex main/survivable core template.

When you restore the upgrade dataset, on the Server Role Web page, the system automatically populates the following fields:

- **Server role**
- **SID**
- **MID**
- **Memory Setting**

In all the blank fields, enter the values manually using this worksheet.

Note:

IPv6 has restricted usage. Therefore, unless instructed otherwise, keep IPv6 disabled and do not enter 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 must 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, assign *1* to one server and *2* to the other server.

For duplicated survivable core server, 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, on the Network Configuration Web page, the system automatically populates the following fields:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values manually using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

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 must 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 configured **CM Hostname** on the System Platform Web Console: • As an FQDN, the Web page automatically populates this field in Communication Manager. • As simple hostname, you can configure this

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			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 you configured **Domain Search List** on System Platform, the system automatically populates the **Domain Search List** field in Communication Manager. If you did not configure the **Search Domain list 1** 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**	-

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
Primary DNS		**Configure Server > DNS**	Entered on the System Platform Web Console at the time of installation
Secondary DNS		**Configure Server > DNS**	Entered on the System Platform Web Console 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 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. You use this IP address in another field.
eth0 mask 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 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	-
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

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
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
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

Server ID for a server must be unique. 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, assign *1* to one server and *2* to the other server.

For duplicated survivable core server, the server ID on the Network Configuration Web page must also correspond to Communication Manager translations on the corresponding survivable-processor SAT screen. For more information on administering Communication Manager for survivable processors, see *Avaya Aura™ Communication Manager Survivability Options*, 03-603633.

When you restore the upgrade dataset, on the Network Configuration Web page, the system automatically populates the following information:

- **eth0 functional assignment**
- **Server ID**

In all the blank fields, enter the values manually using this worksheet.

When you restore the upgrade dataset, the system automatically populates the following fields from the System Platform settings:

- **Host Name**
- **Gateway and Mask**
- **IP addresses**

Enter the values in the fields on one of the following interfaces:

- System Management Interface:
  - **DNS Domain**
  - **Domain Search List**
  - **DNS**
- System Platform Web Console, **Server Management** > **Network Configuration**.

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 must 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 this host name in another field.

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
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 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 **Domain Search List** 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 you configured **Domain Search List** on System Platform, the **Domain Search List** field is automatically populated in Communication Manager. If you did not **Search Domain list 1** configure on System Platform, you can configure the **Search**

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
			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**	-
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. Populated during the installation of Communication Manager template.

Field	Value	Method for obtaining from CM Release 5.2.1	Note
			Use the IP address assigned for server 1. Do not use the IP address of the Communication Manager Release 5.2.1 server. You use this IP address in another field.
eth0 mask IPv4		**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, 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 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

Field	Value	Method for obtaining from CM Release 5.2.1	Notes
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, the system populates during the installation of Communication Manager template.
eth1 Alias IP address	Leave this field blank	**Configure Server > Configure Interfaces**	Leave the 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.
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.

Field	Value	Notes
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 6.2.1, 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 6.2.1.
- Port networks with duplicated IPSI circuit pack (HP DL360 G7 or Dell R610 Server in duplex configuration).
- Port networks with simplex IPSI circuit pack.

Preparing for port network conversion

Procedure

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

Before you begin

- IPSIs are running the latest available firmware.
- DHCP service for private control networks is disabled on Communication Manager servers.
- SAT session is started.

About this task

Convert the duplicated IPSI systems on the public control network to control network C.

Procedure

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
8	Administering PN synchronization

#	Task
9	Completing post-conversion tasks

Changing synchronization

About this task

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.

Procedure

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

Procedure

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

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

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 also adjust the administration of the network regions. Your planning documents provide the information about changes to network regions. For more information on how to administer the 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 pack

Before you begin

Start a SAT session.

About this task

Perform Step 1 and Step 2 only once for all IPSIs. Repeat Step 3 for each IPSI.

Procedure

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

About this task

For static addressing, perform the steps on the circuit pack:

Procedure

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

Before you begin

Start a SAT session.

Procedure

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

Procedure

1. Enter `list ipserver-interface`.
2. Verify that the IPSI circuit packs are translated.

   The system displays `0.0.0.0` in the **State of Health - C P E G** field for each healthy IPSI. If the system displays `1` in any position, troubleshoot the problem.

The pattern `0.1.1.0` indicates that a cabinet type is administered incorrectly or a connectivity problem such as an incorrectly terminated cable exists.

Verifying IPSI connectivity

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Diagnostics** > **Ping**.
3. In the **Endpoints to Ping** section, select **IPSIs with cab number (1–99) ___ carrier number** ___.
4. Enter the correct gateway numbers in the text boxes.
5. Click **Execute Ping**.
6. Verify that the endpoints respond correctly.

Administering the media processor circuit pack

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

Procedure

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

About this task

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).

Procedure

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

Before you begin

Start a SAT session.

About this task

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.

Procedure

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

About this task

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.

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

About this task

Complete these steps for each PN that you are converting to IP-PNC:

Procedure

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

Before you begin

Start a SAT session.

About this task

Perform this procedure if the PN that you just converted to IP-PNC requires a synchronization source.

Procedure

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 in the **Circuit Packs Available for Synchronization** section.

5. Obtain a location for the synchronization source circuit pack from the list in the **Circuit Packs Available for Synchronization** section for **Primary** and **Secondary** fields. Select a synchronization source that works.
6. In the **Primary** field, enter the location of a synchronization-source circuit pack.
7. Optionally, in the **Secondary** field, add another location for synchronization-source circuit pack.
8. Press `Submit`.

   Wait for 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 all`.
11. To check for errors, enter `test synchronization port-network n long`.

    The ports listed must display PASS in the **Results** field. If the **Results** field does not display PASS, troubleshoot the synchronization error.

Index

A

accessing 799
the server 799
Accessing 687, 729, 865, 1039
the new server 687, 729, 865, 1039
accessing System Management Interface 1220, 1405, 1616
Accessing the first new server 687, 729, 865, 1039
accessing the server 799
Activating 73
connection preservation during an upgrade 73
Activating connection preservation during an upgrade 73
add 403, 592, 1083, 1488, 1522, 1556, 1604, 1649
add new circuit packs ...399, 586, 1079, 1484, 1517, 1551, 1599, 1644, 1700
adding ...233, 401, 475, 588, 1081, 1486, 1520, 1553, 1601, 1647, 1703
cables for new circuit packs 401, 588, 1081, 1486, 1520, 1553, 1601, 1647, 1703
memory modules 233, 475
adding a branch gateway ...1117, 1242, 1284, 1347, 1414, 1434
adding a third hard drive 234, 476
adding cables for new circuit packs 401, 588, 1081, 1486, 1520, 1553, 1601, 1647, 1703
adding IPSI information 403, 592, 1083, 1488, 1522, 1556, 1604, 1649
Adding memory modules 233, 475
addition 399, 586, 1079, 1484, 1517, 1551, 1599, 1644, 1700
of new circuit packs 399, 586, 1079, 1484, 1517, 1551, 1599, 1644, 1700
administering 398, 404, 405, 407, 586, 593–595, 1078, 1084–1086, 1483, 1488, 1490, 1491, 1517, 1524, 1525, 1550, 1558, 1559, 1598, 1601, 1605, 1644, 1651, 1652, 1703, 1707, 1708
C-LAN circuit pack ..407, 595, 1086, 1491, 1525, 1559, 1605, 1652, 1708
media processor circuit pack ...405, 594, 1085, 1490, 1524, 1558, 1651, 1707
new circuit packs 404, 593, 1084, 1488, 1703
the gateway 1601
the IPSIs 398, 586, 1078, 1483, 1517, 1550, 1598, 1644
Administering . 400, 404, 587, 593, 1079, 1084, 1484, 1489, 1518, 1522, 1552, 1557, 1600, 1604, 1645, 1650, 1701, 1704
the IPSI circuit pack 404, 593, 1084, 1489, 1522, 1557, 1604, 1650, 1704
the IPSI circuit packs 400, 587, 1079, 1484, 1518, 1552, 1600, 1645, 1701, 1704
administering new circuit packs 404, 593, 1084, 1488, 1703
Administering PN synchronization . .408, 597, 1088, 1711
administering the C-LAN circuit pack 407, 595, 1086, 1491, 1525, 1559, 1605, 1652, 1708
Administering the for server A for each 822
duplex survivable core 822
node name 822
Administering the gateway 1601
Administering the IPSI circuit pack ..404, 593, 1084, 1489, 1522, 1557, 1604, 1650, 1704
Administering the IPSI circuit packs 400, 587, 1079, 1484, 1518, 1552, 1600, 1645, 1701, 1704
administering the IPSIs . 398, 586, 1078, 1483, 1517, 1550, 1598, 1644
administering the media processor circuit pack 405, 594, 1085, 1490, 1524, 1558, 1651, 1707
Administering the node name for server A for each duplex survivable core 822
Administering the signaling group for Communication Manager and Communication Manager Messaging 205, 247, 295, 334, 370, 396, 1121, 1170, 1208, 1247, 1289, 1326, 1481, 1515, 1548, 1594, 1640
alarm activation level ...407, 596, 1087, 1123, 1349, 1492, 1525, 1560, 1606, 1652
announcement sets 48, 116, 189, 227, 271, 317, 355, 1143, 1191, 1229, 1271, 1310, 1578, 1625
application data 48, 115, 189, 226, 270, 316, 354, 1143, 1190, 1228, 1270, 1310, 1577, 1624
authentication 154, 628, 785, 1155
authentication files 26
about 26
Avaya Mentor videos 19
Avaya S8xxx Servers 40, 55, 66, 74, 83, 89, 96, 101, 108, 123, 134, 157, 166, 179, 198, 216, 240, 259, 288, 306, 327, 344, 363, 390, 420, 429, 438, 453, 463, 483, 493, 516, 526, 542, 551, 567, 589, 608, 631, 640, 644, 657, 667, 683, 699, 710, 725, 741, 752, 766, 780, 789, 793, 809, 816, 819, 835, 846, 860, 876, 888, 898, 920, 925, 942, 946, 952, 960, 970, 982, 987, 994, 999, 1004, 1012, 1022, 1035, 1051, 1069, 1077, 1113, 1132, 1149, 1163, 1181, 1201, 1238, 1260, 1280, 1300, 1319, 1353, 1359,

1370, 1378, 1394, 1415, 1425, 1435, 1442, 1456, 1475, 1509, 1542, 1568, 1586, 1633
accessing System Management Interface ..157, 166, 631, 780, 789, 793
accessing the Maintenance Web Interface 134, 420, 608, 644, 752, 766, 1359
accessing the System Management Interface 40, 55, 66, 74, 83, 89, 96, 101, 108, 123, 179, 198, 216, 240, 259, 288, 306, 327, 344, 363, 390, 429, 438, 453, 463, 483, 493, 516, 526, 542, 551, 567, 589, 640, 657, 667, 683, 699, 710, 725, 741, 809, 816, 819, 835, 846, 860, 876, 888, 898, 920, 925, 942, 946, 952, 960, 970, 982, 987, 994, 999, 1004, 1012, 1022, 1035, 1051, 1069, 1077, 1113, 1132, 1149, 1163, 1181, 1201, 1238, 1260, 1280, 1300, 1319, 1353, 1370, 1378, 1394, 1415, 1425, 1435, 1442, 1456, 1475, 1509, 1542, 1568, 1586, 1633

B

backed up files 189, 226, 270, 316, 354, 448, 472, 501, 536, 562, 677, 719, 846, 854, 897, 905, 970, 977, 1022, 1029, 1142, 1158, 1190, 1228, 1270, 1310, 1388, 1451, 1577, 1624
backing 48, 115, 189, 226, 270, 316, 354, 1143, 1190, 1228, 1270, 1310, 1577, 1624
Communication Manager Messaging application data ...48, 115, 189, 226, 270, 316, 354, 1143, 1190, 1228, 1270, 1310, 1577, 1624
backing up 45, 60, 71, 78, 99, 104, 113, 128, 174, 211, 253, 301, 339, 377, 414, 434, 460, 489, 522, 548, 573, 602, 650, 693, 704, 735, 746, 825, 830, 870, 881, 950, 955, 1003, 1007, 1045, 1056, 1096, 1100, 1128, 1177, 1214, 1253, 1296, 1332, 1355, 1376, 1401, 1419, 1439, 1462, 1495, 1528, 1562, 1610, 1656
System Platform and solution template ...45, 60, 71, 78, 99, 104, 113, 128, 174, 211, 253, 301, 339, 377, 414, 434, 460, 489, 522, 548, 573, 602, 650, 693, 704, 735, 746, 825, 830, 870, 881, 950, 955, 1003, 1007, 1045, 1056, 1096, 1100, 1128, 1177, 1214, 1253, 1296, 1332, 1355, 1376, 1401, 1419, 1439, 1462, 1495, 1528, 1562, 1610, 1656
Backing up ..46, 49, 114, 117, 139, 145, 146, 158, 185, 188, 190, 192, 222, 225, 228, 229, 265, 269, 272, 273, 312, 315, 318, 320, 350, 353, 356, 357, 423, 444, 447, 468, 471, 498, 500, 532, 535, 557, 561, 613, 614, 619, 621, 632, 674, 676, 716, 718, 757, 762, 763, 769, 773, 775, 801, 842, 845, 850, 853, 894, 896, 901, 904, 966, 969, 973, 976, 1019, 1021, 1026, 1028, 1138, 1141, 1144, 1146, 1157, 1187, 1189, 1192, 1193, 1224, 1227, 1230, 1231, 1266, 1269, 1272, 1273, 1306, 1309, 1311, 1313, 1363, 1384, 1387, 1407, 1426, 1447, 1450, 1574, 1576, 1579, 1580, 1620, 1623, 1626, 1627
files to a flashcard 145, 613, 619, 762, 773
files to another server 49, 117, 139, 185, 190, 192, 222, 228, 229, 265, 272, 273, 312, 318, 320, 350, 356, 357, 423, 444, 468, 498, 532, 557, 614, 674, 716, 757, 769, 842, 850, 894, 901, 966, 973, 1019, 1026, 1144, 1146, 1187, 1192, 1193, 1230, 1231, 1266, 1272, 1273, 1306, 1311, 1313, 1363, 1384, 1426, 1447, 1574, 1579, 1580, 1626, 1627
files to server 46, 114
the files 1138, 1141, 1224, 1407, 1620
to localhost 146, 158, 621, 632, 763, 775
using Linux migration procedure ..188, 225, 269, 315, 353, 447, 471, 500, 535, 561, 676, 718, 801, 845, 853, 896, 904, 969, 976, 1021, 1028, 1157, 1189, 1227, 1269, 1309, 1387, 1450, 1576, 1623
Backing up CM Messaging data ...62, 129, 212, 255, 302, 340, 378, 415, 1129, 1178, 1215, 1254, 1297, 1334, 1496, 1529, 1564, 1611, 1658
Backing up Communication Manager 44, 70, 76, 112, 139, 184, 221, 265, 312, 349, 423, 443, 468, 497, 531, 557, 613, 673, 716, 756, 769, 841, 849, 893, 901, 966, 973, 1018, 1026, 1137, 1186, 1224, 1266, 1305, 1363, 1384, 1406, 1426, 1447, 1574, 1620
Backing up the files 1138, 1141, 1224, 1407, 1620
Backing up the files to restore 188, 225, 269, 315, 353, 447, 471, 500, 535, 561, 676, 718, 801, 845, 853, 896, 904, 969, 976, 1021, 1028, 1157, 1189, 1227, 1269, 1309, 1387, 1450, 1576, 1623
Backing up to localhost 146, 158, 621, 632, 763, 775
backing up using Linux migration procedure 188, 225, 269, 315, 353, 447, 471, 500, 535, 561, 676, 718, 801, 845, 853, 896, 904, 969, 976, 1021, 1028, 1157, 1189, 1227, 1269, 1309, 1387, 1450, 1576, 1623
backing up, . .44, 70, 76, 112, 139, 184, 221, 265, 312, 349, 423, 443, 468, 497, 531, 557, 613, 673, 716, 756, 769, 841, 849, 893, 901, 966, 973, 1018, 1026, 1137, 1186, 1224, 1266, 1305, 1363, 1384, 1406, 1426, 1447, 1574, 1620
destinations . .44, 70, 76, 112, 139, 184, 221, 265, 312, 349, 423, 443, 468, 497, 531, 557, 613, 673, 716, 756, 769, 841, 849, 893, 901, 966, 973, 1018, 1026, 1137, 1186, 1224, 1266, 1305, 1363, 1384, 1406, 1426, 1447, 1574, 1620

the data ..44, 70, 76, 112, 139, 184, 221, 265, 312, 349, 423, 443, 468, 497, 531, 557, 613, 673, 716, 756, 769, 841, 849, 893, 901, 966, 973, 1018, 1026, 1137, 1186, 1224, 1266, 1305, 1363, 1384, 1406, 1426, 1447, 1574, 1620
backup data 1153
book organization 16, 35
busy out 79, 90, 814, 1074
busying out 58, 97, 126, 172, 299, 374, 648, 690, 732, 823, 867, 948, 1000, 1042, 1094, 1174, 1212, 1251, 1294, 1330, 1608, 1655
busied-out equipment 58, 97, 126, 172, 299, 374, 648, 690, 732, 823, 867, 948, 1000, 1042, 1094, 1174, 1212, 1251, 1294, 1330, 1608, 1655
busying out previously busied-out equipment 58, 97, 126, 172, 299, 374, 648, 690, 732, 823, 867, 948, 1000, 1042, 1094, 1174, 1212, 1251, 1294, 1330, 1608, 1655
busying out server 79, 90, 814, 1074

C

changing synchronization 1700
check 42, 43, 57, 68, 69, 110, 125, 171, 183, 208, 220, 250, 251, 263, 264, 298, 310, 311, 336, 348, 349, 373, 412, 432, 443, 457, 467, 487, 497, 520, 531, 545, 555, 556, 571, 601, 647, 648, 672, 689, 714, 731, 798, 799, 813, 821, 822, 840, 841, 867, 892, 893, 964, 965, 1017, 1042, 1074, 1093, 1127, 1173, 1174, 1211, 1250, 1251, 1264, 1265, 1293, 1294, 1305, 1329, 1352, 1374, 1383, 1399, 1417, 1437, 1446, 1461, 1494, 1527, 1561, 1607, 1608, 1654
translation corruption ...43, 57, 69, 110, 125, 171, 183, 208, 220, 250, 264, 298, 311, 336, 349, 373, 412, 432, 443, 457, 467, 487, 497, 520, 531, 545, 556, 571, 601, 647, 672, 689, 714, 731, 798, 799, 813, 821, 841, 867, 893, 965, 1017, 1042, 1074, 1093, 1127, 1173, 1211, 1250, 1265, 1293, 1305, 1329, 1352, 1374, 1383, 1399, 1417, 1437, 1446, 1461, 1494, 1527, 1561, 1607, 1654
Checking 149, 624, 780, 1132, 1148, 1184, 1358, 1381, 1571
availability of the FTP, SFTP, or SCP server 1132, 1184, 1358, 1381, 1571
the reboot progress 149, 624, 780, 1148
Checking clock synchronization 42, 68, 110, 183, 220, 263, 310, 348, 555, 672, 714, 840, 892, 964, 1017, 1264
Checking for backed up files 189, 226, 270, 316, 354, 448, 472, 501, 536, 562, 677, 719, 846, 854, 897, 905, 970, 977, 1022, 1029, 1142, 1158, 1190, 1228, 1270, 1310, 1388, 1451, 1577, 1624
checking for IP address 1155
checking for the CMM IP address 1155
Checking hardware 223, 267, 351, 499, 559, 897, 906
on the server 223, 267, 351, 499, 559, 897, 906
checking media modules ..171, 251, 648, 822, 1093, 1174, 1211, 1251, 1294, 1329, 1608, 1654
Checking the reboot progress 149, 624, 780, 1148
checklist ..177, 215, 257, 437, 462, 491, 525, 606, 834, 886, 1699
conversion tasks 1699
onsite server upgrade ...177, 215, 257, 437, 462, 491, 525, 606, 834, 886
checklist, ...38, 64, 106, 177, 305, 342, 381, 436, 524, 550, 576, 606, 666, 708, 751, 833, 885, 958, 1011, 1060, 1104, 1218, 1258, 1338, 1403, 1423, 1466, 1499, 1532, 1567, 1614, 1699
Preconversion checklist 1699
Presite upgrade ..38, 64, 106, 177, 305, 342, 436, 524, 550, 606, 666, 708, 751, 833, 885, 958, 1011, 1567, 1614
preupgrade 381, 576, 1060, 1466, 1499, 1532
Preupgrade checklist ...1104, 1218, 1258, 1338, 1403, 1423
circuit packs 403, 592, 1083
Clearing ..134, 420, 608, 644, 752, 766, 789, 793, 797, 816, 818, 1076, 1359
the ARP cache on the laptop computer 134, 420, 608, 644, 752, 766, 789, 793, 797, 816, 818, 1076, 1359
Clearing alarms ...41, 67, 76, 109, 137, 181, 218, 262, 309, 347, 441, 466, 496, 529, 554, 611, 671, 713, 754, 839, 891, 963, 1015, 1135, 1184, 1221, 1263, 1303, 1382, 1445, 1571, 1617
Clearing the ARP cache on the laptop computer 134, 420, 608, 644, 752, 766, 789, 793, 797, 816, 818, 1076, 1359
clock synchronization 42, 68, 110, 183, 220, 263, 310, 348, 555, 672, 714, 840, 892, 964, 1017, 1264
CMM 1155
cold standby server 1140
Communication Manager 20, 1679
upgrades 20
Communication Manager Messaging data ..61, 129, 212, 254, 302, 340, 378, 415, 1129, 1178, 1215, 1254, 1297, 1333, 1496, 1529, 1564, 1611, 1657
Communication Manager Messaging IP address ...1155
Communication Manager survivable servers 24
Communication Manager template 22
Communication Manager upgrade 304, 342, 549
Completing connections on staged servers 803
duplication cable 803

Completing duplication cable connections on staged servers 803
Completion tasks on the staged server 788, 792, 796
configurations 1697
configure 168, 201, 242, 290, 329, 365, 456, 485, 518, 544, 569, 1166, 1203, 1240, 1282, 1321, 1372, 1397, 1458, 1589, 1635
server data 168, 201, 242, 290, 329, 365, 456, 485, 518, 544, 569, 1166, 1203, 1240, 1282, 1321, 1372, 1397, 1458, 1589, 1635
Configure 643, 659, 685, 701, 727, 743, 811, 862, 878, 922, 944, 984, 996, 1037, 1053, 1072
server data 643, 659, 685, 701, 727, 743, 811, 862, 878, 922, 944, 984, 996, 1037, 1053, 1072
Configure server data ...168, 201, 242, 290, 329, 365, 456, 485, 518, 544, 569, 643, 659, 685, 701, 727, 743, 811, 862, 878, 922, 944, 984, 996, 1037, 1053, 1072, 1166, 1203, 1240, 1282, 1321, 1372, 1397, 1458, 1589, 1635
Configuring 430, 1152, 1372, 1397, 1459
network parameters 1152
server data 430, 1372, 1397, 1459
configuring a branch gateway 1116, 1241, 1283, 1347, 1413, 1433
configuring Communication Manager Release 1109, 1234, 1276, 1471, 1505, 1538, 1582, 1629
configuring Communication Manager Release 6.0 . .386, 581
configuring Communication Manager Release 6.x . .194, 237, 283, 322, 359, 804, 915, 936, 989, 1159, 1196, 1315
Configuring network parameters 1152
Configuring server data 430, 1372, 1397, 1459
Configuring switch link 207, 249, 296, 335, 372, 397, 1122, 1172, 1209, 1249, 1291, 1327, 1482, 1516, 1549, 1595, 1641
configuring the System Platform 194, 237, 283, 322, 359, 386, 581, 804, 915, 936, 989, 1109, 1159, 1196, 1234, 1276, 1315, 1471, 1505, 1538, 1582, 1629
connect cables to new server 679, 721, 805, 1031
connect cables to server 653, 698, 740, 856, 875, 937, 990, 1050
connect cables to the server 156, 630
connect service computer to server 87, 95, 101, 161, 635, 925, 946, 952, 987, 998, 1004
connecting 384, 399, 579, 587, 1063, 1079, 1106, 1219, 1340, 1405, 1469, 1484, 1502, 1518, 1535, 1551, 1599, 1615, 1645, 1701
to the processor 384, 579, 1063, 1106, 1340, 1469, 1502, 1535
to the server . .399, 587, 1079, 1219, 1405, 1484, 1518, 1551, 1599, 1615, 1645, 1701
Connecting . . .169, 401, 589, 645, 688, 729, 779, 820, 827, 1040, 1081, 1092, 1098, 1486, 1520, 1553, 1601, 1647, 1703
the circuit pack cables 401, 589, 1081, 1486, 1520, 1553, 1601, 1647, 1703
the laptop 779
the server to network 169, 645, 688, 729, 820, 827, 1040, 1092, 1098
to the server port 779
connecting cables to the server . .156, 630, 653, 679, 698, 721, 740, 805, 856, 875, 937, 990, 1031, 1050
Connecting Ethernet cables to the Ethernet port 791, 795
Connecting the cables to the Ethernet switch ...383, 578, 1062, 1468, 1501, 1534, 1597, 1642
Connecting the circuit pack cables ..401, 589, 1081, 1486, 1520, 1553, 1601, 1647, 1703
Connecting the laptop to the server port 779
Connecting the server to network 169, 645, 688, 729, 820, 827, 1040, 1092, 1098
Connecting to the 791, 795
Ethernet cables 791, 795
Ethernet port 791, 795
connecting to the processor ...384, 579, 1063, 1106, 1340, 1469, 1502, 1535
connecting to the server 399, 587, 1079, 1484, 1518, 1551, 1599, 1645, 1701
conversion tasks checklist 1699
convert port network 1693
Converting 236, 478
the disk array to RAID 5 .....236, 478
Converting control network 1694
Converting fiber PNs to IP-PNC 758, 843
Converting PNs to IP-PNC 1697
overview 1697
Converting the 282, 510, 914, 935
disk array to RAID 5 .....282, 510, 914, 935
Converting the disk array to RAID 5 ...282, 510, 914, 935
Converting the disk array to RAID 5 (if required) 236, 478
copy 180, 203, 217, 245, 261, 292, 308, 331, 345, 368, 395, 440, 465, 494, 528, 553, 669, 711, 837, 848, 889, 900, 962, 972, 1013, 1024, 1120, 1168, 1182, 1205, 1245, 1261, 1287, 1301, 1324, 1380, 1443, 1480, 1513, 1547, 1570, 1591, 1638
the configuration screens 180, 217, 261, 308, 345, 440, 465, 494, 528, 553, 669, 711, 837, 848, 889, 900, 962, 972, 1013, 1024, 1182, 1261, 1301, 1380, 1443, 1570
copy files to the server 641, 810

copy language packages 203, 245, 292, 331, 368, 395, 1120, 1168, 1205, 1245, 1287, 1324, 1480, 1513, 1547, 1591, 1638
copying ...135, 180, 217, 260, 307, 345, 421, 439, 464, 494, 527, 552, 609, 668, 711, 753, 767, 837, 848, 889, 899, 961, 971, 1013, 1023, 1134, 1182, 1261, 1301, 1360, 1380, 1443, 1569
configuration information System Management Interface ...135, 180, 217, 260, 307, 345, 421, 439, 464, 494, 527, 552, 609, 668, 711, 753, 767, 837, 848, 889, 899, 961, 971, 1013, 1023, 1134, 1182, 1261, 1301, 1360, 1380, 1443, 1569
copying configuration information 135, 180, 217, 260, 307, 345, 421, 439, 464, 494, 527, 552, 609, 668, 711, 753, 767, 837, 848, 889, 899, 961, 971, 1013, 1023, 1134, 1182, 1261, 1301, 1360, 1380, 1443, 1569
copying files ...142, 151, 166, 186, 224, 268, 314, 352, 391, 446, 470, 499, 533, 559, 616, 625, 675, 717, 759, 770, 781, 844, 851, 895, 903, 967, 974, 1019, 1027, 1070, 1114, 1138, 1151, 1188, 1226, 1239, 1268, 1281, 1307, 1386, 1449, 1476, 1510, 1543, 1575, 1587, 1622, 1634
server 151, 625, 781, 1138
copying files to the server ...142, 151, 186, 224, 268, 314, 352, 391, 446, 470, 499, 533, 559, 616, 625, 675, 717, 759, 770, 781, 844, 851, 895, 903, 967, 974, 1019, 1027, 1070, 1114, 1138, 1151, 1188, 1226, 1239, 1268, 1281, 1307, 1386, 1449, 1476, 1510, 1543, 1575, 1587, 1622, 1634
Copying files to the server 641, 810
copying the upgrade dataset 166
courses 19
cover 275, 502, 907, 927
removing 275, 502, 907, 927
custom announcements 204, 246, 293, 332, 369, 1169, 1206, 1246, 1288, 1325, 1592, 1639

D

date 1150
decommissioning the cabinet 1124
decommissioning the PPN 1090
DEFINITY CSI 1103
DEFINITY R 1059
DEFINITY Server CSI in a CMC to port network 1465
DEFINITY SI 379, 575, 1059, 1103, 1337
DIMM air baffle 276, 279, 504, 507, 908, 911, 929, 932
installing 279, 507, 911, 932
removing 276, 504, 908, 929
DIMMs 277, 505, 909, 930
installing 277, 505, 909, 930
direct connection 788, 792, 796, 815, 818, 1076
Disabling 43, 69, 111, 140, 183, 220, 264, 311, 348, 442, 530, 556, 615, 673, 715, 758, 840, 892, 965, 1018, 1088, 1137, 1185, 1223, 1264, 1304, 1573, 1619, 1710
PNC duplication 1088, 1710
scheduled maintenance ...43, 69, 111, 140, 183, 220, 264, 311, 348, 442, 530, 556, 615, 673, 715, 758, 840, 892, 965, 1018, 1137, 1185, 1223, 1264, 1304, 1573, 1619
Disabling PNC duplication 1088, 1710
discard the cabinet 416, 603, 1131, 1255, 1298, 1356, 1420, 1440
discard the circuit packs 416, 603, 1131, 1255, 1298, 1356, 1420, 1440
disconnect 231, 473
the cables 231, 473
disconnecting 63, 74, 86, 95, 100, 105, 131, 148, 193, 213, 256, 275, 303, 321, 341, 359, 379, 409, 416, 425, 448, 461, 490, 502, 523, 536, 549, 562, 574, 598, 603, 622, 677, 719, 765, 777, 803, 846, 898, 907, 924, 927, 946, 951, 957, 970, 977, 986, 989, 998, 1004, 1009, 1022, 1029, 1039, 1089, 1123, 1130, 1195, 1256, 1292, 1314, 1356, 1364, 1389, 1421, 1441, 1452, 1492, 1497, 1530, 1565, 1582, 1596, 1643
from the server 63, 74, 86, 95, 100, 105, 131, 213, 256, 303, 341, 379, 409, 416, 461, 490, 523, 549, 574, 598, 603, 924, 927, 946, 951, 957, 986, 989, 998, 1004, 1009, 1089, 1123, 1130, 1292, 1356, 1441, 1492, 1497, 1530, 1565
the cables 193, 275, 321, 359, 448, 502, 536, 562, 898, 907, 970, 977, 1039
the devices 1195, 1314, 1364, 1389, 1452
the portable computer from the server 148, 425, 622, 677, 719, 765, 777, 803, 846, 1022, 1029, 1256, 1421, 1582, 1596, 1643
disconnecting modem 1195, 1364, 1389
disconnecting USB CD/DVD reader 1314, 1452
document purpose 15
Documentation checklist ..38, 64, 178, 215, 258, 305, 343, 381, 437, 462, 492, 525, 550, 577, 607, 666, 708, 751, 834, 885, 959, 1011, 1061, 1104, 1218, 1259, 1338, 1404, 1423, 1467, 1500, 1533, 1568, 1615
documentation required 34
Downloading remote field update 202, 244, 291, 330, 367, 394, 1118, 1167, 1204, 1244, 1286, 1322, 1479, 1512, 1546, 1590, 1636
duplex CM main/survivable template 605
duplex main/survivable core template 1059

Duplex main/survivable core template 678, 720, 1030
duplex main/survivable template 63, 884, 958
duplicated server 26
licensing 26
duplication cable 854
duplication parameters 643, 659, 685, 701, 727, 743, 811, 862, 878, 922, 944, 984, 996, 1037, 1053, 1072
DVD/CD-ROM drive 1357

E

embedded main template 105, 1103
embedded survivable remote template 1337
enabe FTP service 146, 158, 620, 632, 763, 774, 801
enable 58, 97, 125, 146, 158, 171, 251, 298, 374, 620, 632, 648, 690, 732, 763, 774, 801, 823, 867, 948, 1000, 1042, 1094, 1174, 1211, 1251, 1294, 1330, 1608, 1655
FTP service 146, 158, 620, 632, 763, 774, 801
scheduled maintenance ...58, 97, 125, 171, 251, 298, 374, 648, 690, 732, 823, 867, 948, 1000, 1042, 1094, 1174, 1211, 1251, 1294, 1330, 1608, 1655
Enabling 137, 423, 611, 755, 768, 1221, 1617
Telnet service 137, 423, 611, 755, 768, 1221, 1617
Enabling Telnet service 137, 423, 611, 755, 768, 1221, 1617
error message 798
existing hardware 382, 577, 1061, 1468, 1501, 1534, 1597, 1642
Existing hardware upgrade ...382, 577, 1061, 1468, 1501, 1534, 1597, 1642
external references 16

F

Fiber-PNC configurations 1697
Fiber-PNC 1697
firmware upgrade 402, 591, 1082, 1487, 1521, 1556, 1603, 1648, 1709
flashcard 145, 619, 762, 773
front benzel 231, 473
front bezel 235, 477
FTP, SFTP, or SCP 1132, 1184, 1358, 1381, 1571

H

hard disk drive 280, 508, 912, 933
installing 280, 508, 912, 933
high-level tasks 750

I

identify ..48, 116, 189, 227, 271, 317, 355, 1144, 1191, 1229, 1271, 1311, 1578, 1625
language packages ..48, 116, 189, 227, 271, 317, 355, 1144, 1191, 1229, 1271, 1311, 1578, 1625
identify the language packages 48, 116, 189, 227, 271, 317, 355, 1144, 1191, 1229, 1271, 1311, 1578, 1625
Identifying 790, 794
the Ethernet interface 790, 794
Identifying the Ethernet interface 790, 794
Inserting 777
Communication Manager disc 777
Inserting Communication Manager disc 777
install 172, 209, 252, 299, 337, 375, 413, 433, 520, 571, 601, 649, 661, 691, 703, 733, 745, 824, 829, 868, 880, 948, 953, 1001, 1005, 1043, 1055, 1095, 1099, 1127, 1175, 1212, 1252, 1295, 1331, 1353, 1375, 1399, 1418, 1438, 1461, 1494, 1527, 1562, 1609, 1656
phone message file 172, 209, 252, 299, 337, 375, 413, 433, 520, 571, 601, 649, 661, 691, 703, 733, 745, 824, 829, 868, 880, 948, 953, 1001, 1005, 1043, 1055, 1095, 1099, 1127, 1175, 1212, 1252, 1295, 1331, 1353, 1375, 1399, 1418, 1438, 1461, 1494, 1527, 1562, 1609, 1656
Install phone message file ...172, 209, 252, 299, 337, 375, 413, 433, 520, 571, 601, 649, 661, 691, 703, 733, 745, 824, 829, 868, 880, 948, 953, 1001, 1005, 1043, 1055, 1095, 1099, 1127, 1175, 1212, 1252, 1295, 1331, 1353, 1375, 1399, 1418, 1438, 1461, 1494, 1527, 1562, 1609, 1656
install server in rack 235, 476
install the new server 678, 720, 855, 1030, 1065
install the new server in the rack 678, 720, 855, 1030, 1065
installing 161, 194, 237, 283, 322, 359, 386, 399, 425, 449, 478, 511, 538, 563, 581, 586, 635, 652, 678, 694, 720, 736, 804, 855, 871, 915, 936, 978, 989, 1030, 1046, 1065, 1078, 1109, 1159, 1196, 1234, 1276, 1315, 1343, 1366, 1390, 1409, 1429, 1452, 1471, 1505, 1538, 1582, 1599, 1629
G650 Media Gateway in the rack 399, 586, 1078, 1599
Installing 142, 144, 148, 152, 204, 240, 246, 293, 332, 369, 396, 399, 587, 617, 618, 623, 626, 760, 761, 771, 772, 779, 782, 941, 1079, 1108, 1120, 1141, 1147, 1151, 1169, 1206, 1233, 1246, 1275, 1288, 1324, 1341, 1408, 1428, 1481, 1484, 1514, 1518, 1548, 1551, 1592, 1599, 1638, 1645, 1701

a circuit pack . 399, 587, 1079, 1484, 1518, 1551, 1599, 1645, 1701
Communication Manager 148, 623, 779, 1147
language packages 204, 246, 293, 332, 369, 396, 1120, 1169, 1206, 1246, 1288, 1324, 1481, 1514, 1548, 1592, 1638
S8300D Server ...1108, 1233, 1275, 1341, 1408, 1428
service pack ..144, 152, 618, 626, 761, 772, 782, 1151
service pack updates 142, 240, 617, 760, 771, 941
the preupgrade service pack on the server running release 2.0 1141
Installing a circuit pack ..399, 587, 1079, 1484, 1518, 1551, 1599, 1645, 1701
installing Communication Manager . . .161, 425, 449, 478, 511, 538, 563, 635, 652, 678, 694, 720, 736, 855, 871, 978, 1030, 1046, 1065, 1343, 1366, 1390, 1409, 1429, 1452
Installing Communication Manager . .148, 623, 779, 1147
installing G650 Media Gateway in the rack 399, 586, 1078, 1599
Installing preupgrade service pack 142, 617, 1139
Installing Remote Field Update ...202, 244, 291, 330, 367, 394, 1119, 1167, 1204, 1244, 1286, 1323, 1479, 1513, 1546, 1591, 1637
Installing S8300D Server in the gateway 1108, 1233, 1275, 1341, 1408, 1428
Installing service pack . .144, 152, 618, 626, 761, 772, 782, 1151
Installing service pack updates ...142, 240, 617, 760, 771, 941
installing the preupgrade service pack 157, 187, 224, 268, 315, 352, 446, 470, 500, 534, 560, 631, 675, 717, 800, 844, 852, 895, 904, 968, 975, 1020, 1027, 1140, 1157, 1188, 1226, 1268, 1308, 1386, 1449, 1575, 1622
Installing the preupgrade service pack on the server running release 2.0 1141
installing the server in the rack 678, 720, 855, 1030, 1065
Installing the service pack 142, 617, 1139
installing the System Platform 161, 425, 449, 478, 511, 538, 563, 635, 652, 678, 694, 720, 736, 855, 871, 978, 1030, 1046, 1065, 1343, 1366, 1390, 1409, 1429, 1452
intended audience 15
interchange servers 85, 663, 705, 747, 831, 882, 956, 1008, 1058, 1101
Introduction 1693
IP forwarding 39, 65, 75, 87, 107, 162, 195, 237, 284, 323, 360, 387, 426, 450, 479, 512, 538, 563, 582, 636, 653, 679, 695, 721, 737, 805, 856, 872, 916, 937, 978, 990, 1031, 1047, 1066, 1109, 1160, 1197, 1234, 1276, 1315, 1343, 1366, 1391, 1409, 1429, 1453, 1472, 1505, 1538, 1583, 1629
disabling . .39, 65, 75, 87, 107, 162, 195, 237, 284, 323, 360, 387, 426, 450, 479, 512, 538, 563, 582, 636, 653, 679, 695, 721, 737, 805, 856, 872, 916, 937, 978, 990, 1031, 1047, 1066, 1109, 1160, 1197, 1234, 1276, 1315, 1343, 1366, 1391, 1409, 1429, 1453, 1472, 1505, 1538, 1583, 1629
enabling . .39, 65, 75, 87, 107, 162, 195, 237, 284, 323, 360, 387, 426, 450, 479, 512, 538, 563, 582, 636, 653, 679, 695, 721, 737, 805, 856, 872, 916, 937, 978, 990, 1031, 1047, 1066, 1109, 1160, 1197, 1234, 1276, 1315, 1343, 1366, 1391, 1409, 1429, 1453, 1472, 1505, 1538, 1583, 1629
IPSI information . .403, 592, 1083, 1488, 1522, 1556, 1604, 1649

L

label 231, 275, 321, 359, 473, 502, 536, 562, 898, 907, 970, 977, 1039
language packages 48, 116, 189, 203, 204, 227, 245, 246, 271, 292, 293, 317, 331, 332, 355, 368, 369, 395, 396, 1120, 1143, 1144, 1168, 1169, 1191, 1205, 1206, 1229, 1245, 1246, 1271, 1287, 1288, 1310, 1311, 1324, 1480, 1481, 1513, 1514, 1547, 1548, 1578, 1591, 1592, 1625, 1638
legal notice 2
license 154, 628, 785, 1155
license error message 798
licensing 25, 26
about 25
duplicated server 26
localhost 145, 619, 762, 773
Log off 63, 100, 105, 130, 175, 213, 256, 303, 341, 379, 416, 435, 461, 490, 523, 549, 574, 603, 652, 664, 694, 706, 736, 748, 827, 832, 871, 883, 957, 1009, 1046, 1059, 1097, 1102, 1130, 1179, 1216, 1255, 1298, 1335, 1356, 1377, 1402, 1420, 1440, 1463, 1497, 1530, 1565, 1612, 1659
administration applications 63, 100, 105, 130, 175, 213, 256, 303, 341, 379, 416, 435, 461, 490, 523, 549, 574, 603, 652, 664, 694, 706, 736, 748, 827, 832, 871, 883, 957, 1009, 1046, 1059, 1097, 1102, 1130, 1179, 1216, 1255, 1298, 1335, 1356, 1377, 1402, 1420, 1440, 1463, 1497, 1530, 1565, 1612, 1659

M

MBT 304
media modules 171, 251, 648, 822, 1093, 1174, 1211, 1251, 1294, 1329, 1608, 1654
memory module air baffle 276, 279, 504, 507, 908, 911, 929, 932
  installing 279, 507, 911, 932
  removing 276, 504, 908, 929
memory modules 277, 505, 909, 930
  installing 277, 505, 909, 930
Midsize Business Template 304

N

network configuration ...168, 201, 242, 290, 329, 365, 456, 485, 518, 544, 569, 643, 659, 685, 701, 727, 743, 811, 862, 878, 922, 944, 984, 996, 1037, 1053, 1072, 1166, 1203, 1240, 1282, 1321, 1372, 1397, 1458, 1589, 1635
new server 148, 161, 194, 322, 386, 449, 537, 581, 623, 652, 1147, 1471, 1504, 1538, 1582, 1628
node names ..205, 247, 295, 334, 370, 385, 396, 581, 1065, 1121, 1170, 1208, 1223, 1247, 1289, 1326, 1470, 1481, 1503, 1515, 1537, 1548, 1594, 1619, 1640

O

Overview 1697

P

patches ...52, 53, 81, 82, 92, 120, 121, 164, 165, 197, 198, 286, 287, 325, 326, 362, 389, 428, 429, 452, 453, 481, 482, 514, 515, 540, 541, 565, 566, 584, 585, 638, 639, 655, 656, 681, 682, 697, 723, 724, 739, 807, 808, 858, 859, 874, 918, 919, 939, 940, 980, 981, 992, 993, 1033, 1034, 1049, 1050, 1068, 1069, 1111, 1112, 1162, 1163, 1199, 1200, 1236, 1237, 1278, 1279, 1318, 1345, 1346, 1368, 1369, 1393, 1394, 1411, 1412, 1431, 1432, 1455, 1474, 1507, 1508, 1541, 1585, 1586, 1631, 1632
  downloading 52, 81, 92, 120, 164, 197, 286, 325, 362, 389, 428, 452, 481, 514, 540, 565, 584, 638, 655, 681, 697, 723, 739, 807, 858, 874, 918, 939, 980, 992, 1033, 1049, 1068, 1111, 1162, 1199, 1236, 1278, 1318, 1345, 1368, 1393, 1411, 1431, 1455, 1474, 1507, 1541, 1585, 1631
  installing 53, 82, 92, 121, 165, 198, 287, 326, 362, 389, 429, 453, 482, 515, 541, 566, 585, 639, 656, 682, 697, 724, 739, 808, 859, 874, 919, 940, 981, 993, 1034, 1050, 1069, 1112, 1163, 1200, 1237, 1279, 1318, 1346, 1369, 1394, 1412, 1432, 1455, 1474, 1508, 1541, 1586, 1632
Performing 56, 85, 86, 94, 124, 170, 249, 297, 372, 431, 486, 519, 570, 646, 661, 664, 688, 702, 706, 730, 744, 748, 828, 866, 879, 883, 923, 926, 945, 956, 985, 988, 998, 1009, 1041, 1055, 1058, 1099, 1172, 1210, 1249, 1292, 1328, 1373, 1398, 1417, 1437, 1460, 1606, 1653
  an integrity check ...56, 85, 86, 94, 124, 170, 249, 297, 372, 431, 486, 519, 570, 646, 661, 664, 688, 702, 706, 730, 744, 748, 828, 866, 879, 883, 923, 926, 945, 956, 985, 988, 998, 1009, 1041, 1055, 1058, 1099, 1172, 1210, 1249, 1292, 1328, 1373, 1398, 1417, 1437, 1460, 1606, 1653
Performing an integrity 85, 94, 661, 702, 744, 828, 879, 923, 926, 945, 985, 988, 998, 1055, 1099
Performing an integrity check ..56, 86, 124, 170, 249, 297, 372, 431, 486, 519, 570, 646, 664, 688, 706, 730, 748, 866, 883, 956, 1009, 1041, 1058, 1172, 1210, 1249, 1292, 1328, 1373, 1398, 1417, 1437, 1460, 1606, 1653
PN synchronization 408, 597, 1088, 1711
port network circuit packs 403, 592, 1083, 1488, 1522, 1556, 1649
pre-upgrade activation 1140
prepare 777
  the server for the upgrade 777
Preparing for 1693
  port network conversion 1693
Preparing for port network conversion 1693
preparing the server 777
Preupgrade 141, 382, 577, 617, 760, 771, 1061, 1105, 1339, 1467, 1500, 1534
  service packs 141, 617, 760, 771
  setup 382, 577, 1061, 1105, 1339, 1467, 1500, 1534
preupgrade checklist 381, 576, 1060, 1466, 1499, 1532
preupgrade requirements 29
preupgrade service pack 157, 187, 224, 268, 315, 352, 446, 470, 500, 534, 560, 631, 675, 717, 800, 844, 852, 895, 904, 968, 975, 1020, 1027, 1140, 1157, 1188, 1226, 1268, 1308, 1386, 1449, 1575, 1622
Preupgrade service packs 141, 617, 760, 771
Preupgrade setup 382, 577, 1061, 1105, 1339, 1467, 1500, 1534
purpose of document 15

R

rack 321, 537, 1039
removing server 321, 537, 1039
Rebooting the server ...156, 168, 207, 249, 296, 335, 372, 431, 456, 485, 518, 544, 569, 630, 643, 659, 685, 701, 727, 743, 787, 812, 863, 878, 922, 944, 984, 996, 1037, 1053, 1073, 1156, 1172, 1209, 1249, 1291, 1327, 1373, 1398, 1415, 1435, 1459, 1595, 1641
Reconfigure the Communication Manager server 52, 81, 91, 120
Recording 385, 422, 581, 1065, 1142, 1223, 1225, 1362, 1470, 1503, 1504, 1537, 1619, 1621
configuration information 1142, 1225, 1362, 1621
IP settings 1504, 1537
the scheduled backup 422, 1362
Recording all busyouts 42, 68, 110, 138, 182, 219, 263, 310, 348, 385, 555, 580, 612, 672, 714, 756, 840, 892, 964, 1016, 1064, 1107, 1136, 1185, 1222, 1264, 1304, 1341, 1470, 1503, 1536, 1572, 1618
Recording configuration information 1142, 1225, 1362, 1621
Recording IP settings 1504, 1537
Recording node names and IP addresses 385, 581, 1065, 1223, 1470, 1503, 1537, 1619
Registering 63, 105, 131, 175, 213, 256, 341, 417, 435, 604, 664, 707, 749, 832, 884, 957, 1010, 1059, 1102, 1131, 1179, 1216, 1256, 1298, 1335, 1356, 1377, 1402, 1420, 1440, 1463, 1497, 1531, 1565, 1612, 1659
the system 63, 105, 131, 175, 213, 256, 341, 417, 435, 604, 664, 707, 749, 832, 884, 957, 1010, 1059, 1102, 1131, 1179, 1216, 1256, 1298, 1335, 1356, 1377, 1402, 1420, 1440, 1463, 1497, 1531, 1565, 1612, 1659
related resources 15, 19
Avaya Mentor videos 19
release 85, 94, 645, 661, 687, 702, 730, 744, 784, 791, 796, 814, 828, 865, 879, 926, 945, 988, 997, 1040, 1054, 1075, 1098
release 4.0.5 .....148, 623
release 5.2.1 .....148, 623
Release 5.2.1 .....779, 1147
releasing server 85, 94, 645, 661, 687, 702, 730, 744, 784, 791, 796, 814, 828, 865, 879, 926, 945, 988, 997, 1040, 1054, 1075, 1098
releasing the server . .85, 94, 645, 661, 687, 702, 730, 744, 784, 791, 796, 814, 828, 865, 879, 926, 945, 988, 997, 1040, 1054, 1075, 1098
remove ...231, 233, 416, 473, 475, 603, 687, 729, 854, 855, 864, 1131, 1255, 1298, 1356, 1420, 1440
the cabinet and the circuit packs 416, 603, 1131, 1255, 1298, 1356, 1420, 1440
remove from rack 232, 474
remove server from rack 687, 729, 855, 864
Remove the cabinet and the circuit packs 416, 603, 1131, 1255, 1298, 1356, 1420, 1440
remove the front benzel 231, 473
remove the server from the rack 232, 474
Removing ..193, 408, 409, 449, 596, 598, 1087, 1089, 1123, 1124, 1292, 1349, 1350, 1441, 1710, 1711
fiber-related administration 408, 596, 1087, 1123, 1349, 1710
fiber-related hardware 409, 598, 1089, 1124, 1350, 1711
S8500–Series Server from the rack . .193, 449, 1292, 1441
removing duplication cable 854
Removing fiber-related administration 408, 596, 1087, 1123, 1349, 1710
Removing fiber-related hardware ...409, 598, 1089, 1124, 1350, 1711
Removing port network circuit packs 403, 592, 1083, 1488, 1522, 1556, 1649
removing processor port network control cabinet 410, 599, 1091, 1124, 1350
removing S8510 server cover 232, 474
removing the SAMP 233, 475
removing the server 687, 729, 855, 864
replace 234, 235, 476, 477
the S8510 Server cover 234, 476
replace the cover 234, 476
replacing 1554
I/O cables 1554
Replacing 1195, 1365, 1389
a server 1195, 1365, 1389
Replacing a server 1195, 1389
Replacing circuit packs .383, 578, 1062, 1468, 1501, 1535
replacing I/O cables 1554
Replacing S8300A Server 1365
replacing the cover on S8510 server 234, 476
replacing the front bezel 235, 477
required sequence 1180
Resetting the system 799
Resolving ...59, 98, 102, 126, 210, 300, 338, 376, 413, 459, 488, 521, 547, 572, 601, 692, 734, 869, 950, 1002, 1044, 1127, 1354, 1494, 1527, 1562
alarms . .59, 98, 102, 126, 210, 300, 338, 376, 413, 459, 488, 521, 547, 572, 601, 692, 734, 869, 950, 1002, 1044, 1127, 1354, 1494, 1527, 1562

resolving alarms …174, 253, 433, 650, 663, 825, 830, 954, 1007, 1096, 1100, 1176, 1213, 1252, 1295, 1332, 1375, 1400, 1418, 1438, 1462, 1609, 1656
resources 15
restore 1153
Restoring ….155, 167, 200, 204, 205, 241, 246, 247, 289, 293, 294, 328, 332, 333, 364, 369, 370, 392, 455, 484, 517, 543, 568, 629, 642, 658, 684, 700, 726, 742, 786, 810, 861, 877, 921, 943, 983, 995, 1036, 1052, 1071, 1114, 1165, 1169, 1170, 1202, 1206, 1207, 1239, 1246, 1247, 1281, 1288, 1289, 1320, 1325, 1371, 1396, 1457, 1477, 1510, 1544, 1588, 1592, 1593, 1634, 1639
Communication Manager Messaging data . 205, 247, 294, 333, 370, 1170, 1207, 1247, 1289, 1325, 1593, 1639
custom announcements ….204, 246, 293, 332, 369, 1169, 1206, 1246, 1288, 1325, 1592, 1639
server data 155, 629, 786
the translations …..392, 1071, 1114, 1477, 1510, 1544
upgrade dataset ….167, 200, 241, 289, 328, 364, 455, 484, 517, 543, 568, 642, 658, 684, 700, 726, 742, 810, 861, 877, 921, 943, 983, 995, 1036, 1052, 1165, 1202, 1239, 1281, 1320, 1371, 1396, 1457, 1588, 1634
restoring backup data 1153
Resubmitting ..173, 210, 252, 300, 338, 376, 459, 488, 521, 547, 572, 650, 662, 692, 704, 734, 746, 825, 829, 869, 881, 949, 954, 1002, 1006, 1044, 1056, 1095, 1176, 1213, 1331
scheduled backups ….173, 210, 252, 300, 338, 376, 459, 488, 521, 547, 572, 650, 662, 692, 704, 734, 746, 825, 829, 869, 881, 949, 954, 1002, 1006, 1044, 1056, 1095, 1176, 1213, 1331

S

S8100 Server in a CMC to port network 1498
S8100 Server in G600 to port network 1531
S8510 server cover removal 232, 474
S8510 Server on simplex CM main/survivable template 214
S8700 Server upgrade procedure 750
S8700 Server upgrade tasks 750
S8800 server firmware 282, 510, 914, 935
SAMP 233, 475
SAT session ….42, 57, 68, 109, 124, 137, 170, 182, 207, 219, 250, 263, 297, 309, 336, 347, 373, 398, 432, 441, 457, 466, 486, 496, 519, 529, 545, 554, 570, 585, 611, 647, 671, 689, 713, 731, 755, 797, 813, 821, 839, 866, 891, 963, 1016, 1041, 1073, 1093, 1122, 1136, 1173, 1185, 1210, 1222, 1250, 1263, 1293, 1303, 1329, 1349, 1374, 1382, 1399, 1417, 1437, 1446, 1460, 1483, 1516, 1550, 1572, 1598, 1607, 1618, 1643, 1653
save ….44, 58, 70, 97, 111, 126, 172, 208, 251, 299, 312, 337, 349, 374, 383, 412, 443, 458, 467, 497, 531, 546, 557, 578, 648, 672, 690, 715, 732, 756, 798, 823, 841, 867, 893, 948, 966, 1000, 1017, 1043, 1062, 1094, 1105, 1126, 1136, 1175, 1186, 1212, 1223, 1252, 1295, 1305, 1330, 1339, 1383, 1446, 1468, 1501, 1534, 1573, 1609, 1619, 1655
saving 138, 141, 184, 221, 265, 612, 615, 759, 1265
translations ….138, 141, 184, 221, 265, 612, 615, 759, 1265
saving translations ….44, 58, 70, 97, 111, 126, 172, 208, 251, 299, 312, 337, 349, 374, 383, 412, 443, 458, 467, 497, 531, 546, 557, 578, 648, 672, 690, 715, 732, 756, 798, 823, 841, 867, 893, 948, 966, 1000, 1017, 1043, 1062, 1094, 1105, 1126, 1136, 1175, 1186, 1212, 1223, 1252, 1295, 1305, 1330, 1339, 1383, 1446, 1468, 1501, 1534, 1573, 1609, 1619, 1655
second server 795
server ….79, 85, 90, 94, 142, 166, 186, 224, 232, 268, 314, 321, 352, 446, 470, 474, 499, 533, 537, 559, 616, 645, 661, 675, 687, 702, 717, 729, 730, 744, 759, 770, 784, 787, 791, 796, 814, 828, 844, 851, 855, 864, 865, 879, 895, 903, 926, 945, 967, 974, 988, 997, 1019, 1027, 1039, 1040, 1054, 1074, 1075, 1098, 1151, 1156, 1188, 1226, 1268, 1307, 1386, 1449, 1575, 1622
reboot 787, 1156
removing from the rack 321, 537, 1039
server cover 275, 502, 907, 927
removing 275, 502, 907, 927
server duplication cable 795
server role ….168, 201, 242, 290, 329, 365, 456, 485, 518, 544, 569, 643, 659, 685, 701, 727, 743, 811, 862, 878, 922, 944, 984, 996, 1037, 1053, 1072, 1166, 1203, 1240, 1282, 1321, 1372, 1397, 1458, 1589, 1635
servers …40, 55, 66, 74, 83, 85, 89, 96, 101, 108, 123, 134, 157, 166, 179, 198, 216, 240, 259, 288, 306, 327, 344, 363, 390, 420, 429, 438, 453, 463, 483, 493, 516, 526, 542, 551, 567, 589, 608, 631, 640, 644, 657, 663, 667, 683, 699, 705, 710, 725, 741, 747, 752, 766, 780, 789, 793, 809, 816, 819, 831, 835, 846, 860, 876, 882, 888, 898, 920, 925, 942, 946, 952, 956, 960, 970, 982, 987, 994, 999, 1004, 1008, 1012, 1022, 1035, 1051, 1058, 1069, 1077, 1101, 1113, 1132, 1149, 1163, 1181, 1201, 1220, 1238, 1260, 1280, 1300, 1319, 1353, 1359, 1370, 1378,

1394, 1405, 1415, 1425, 1435, 1442, 1456, 1475, 1509, 1542, 1568, 1586, 1616, 1633
accessing System Management Interface ..157, 166, 631, 780, 789, 793, 1220, 1405, 1616
accessing the System Management Interface 40, 55, 66, 74, 83, 89, 96, 101, 108, 123, 134, 179, 198, 216, 240, 259, 288, 306, 327, 344, 363, 390, 420, 429, 438, 453, 463, 483, 493, 516, 526, 542, 551, 567, 589, 608, 640, 644, 657, 667, 683, 699, 710, 725, 741, 752, 766, 809, 816, 819, 835, 846, 860, 876, 888, 898, 920, 925, 942, 946, 952, 960, 970, 982, 987, 994, 999, 1004, 1012, 1022, 1035, 1051, 1069, 1077, 1113, 1132, 1149, 1163, 1181, 1201, 1238, 1260, 1280, 1300, 1319, 1353, 1359, 1370, 1378, 1394, 1415, 1425, 1435, 1442, 1456, 1475, 1509, 1542, 1568, 1586, 1633
interchange 85, 663, 705, 747, 831, 882, 956, 1008, 1058, 1101
service 686, 728, 864, 924, 986, 1038
outage 686, 728, 864, 924, 986, 1038
service outage 686, 728, 864, 924, 986, 1038
services port . .39, 65, 75, 87, 107, 162, 195, 237, 284, 323, 360, 387, 426, 450, 479, 512, 538, 563, 582, 636, 653, 679, 695, 721, 737, 805, 856, 872, 916, 937, 978, 990, 1031, 1047, 1066, 1109, 1160, 1197, 1234, 1276, 1315, 1343, 1366, 1391, 1409, 1429, 1453, 1472, 1505, 1538, 1583, 1629
accessing System Platform through ...39, 65, 75, 87, 107, 162, 195, 237, 284, 323, 360, 387, 426, 450, 479, 512, 538, 563, 582, 636, 653, 679, 695, 721, 737, 805, 856, 872, 916, 937, 978, 990, 1031, 1047, 1066, 1109, 1160, 1197, 1234, 1276, 1315, 1343, 1366, 1391, 1409, 1429, 1453, 1472, 1505, 1538, 1583, 1629
SES 28
set 150, 625, 784
date and time 150, 625, 784
the time, date, and time zone 150, 625, 784
Set Identities 1152
Set the time, date, and time zone 150, 625, 784
set up ...50, 118, 191, 229, 273, 319, 357, 1145, 1193, 1231, 1273, 1312, 1580, 1627
test data ..50, 118, 191, 229, 273, 319, 357, 1145, 1193, 1231, 1273, 1312, 1580, 1627
setting 405, 593, 1084, 1489, 1523, 1557, 1604, 1650, 1705
VLAN parameters and diffserv parameters 405, 593, 1084, 1489, 1523, 1557, 1604, 1650, 1705
setting alarm activation level . .407, 596, 1087, 1123, 1349, 1492, 1525, 1560, 1606, 1652
setting the VLAN parameters and diffserv parameters ... 405, 593, 1084, 1489, 1523, 1557, 1604, 1650, 1705
setting up test data 50, 118, 191, 229, 273, 319, 357, 1145, 1193, 1231, 1273, 1312, 1580, 1627
shut down 50, 118, 191, 229, 273, 319, 357, 1146, 1193, 1231, 1273, 1313, 1580, 1627
Communication Manager Messaging ...50, 118, 191, 229, 273, 319, 357, 1146, 1193, 1231, 1273, 1313, 1580, 1627
Shutting down 50, 118, 191, 229, 273, 319, 357, 1146, 1159, 1193, 1231, 1273, 1313, 1364, 1580, 1627
Communication Manager Messaging ...50, 118, 191, 229, 273, 319, 357, 1146, 1193, 1231, 1273, 1313, 1580, 1627
the server 1159, 1364
Shutting down Communication Manager Messaging 50, 118, 191, 229, 273, 319, 357, 1146, 1193, 1231, 1273, 1313, 1580, 1627
Shutting down the server 160, 169, 193, 230, 274, 321, 358, 425, 445, 472, 502, 536, 562, 634, 645, 686, 728, 803, 817, 820, 854, 864, 906, 924, 977, 986, 1038, 1194, 1256, 1291, 1314, 1388, 1420, 1440, 1451, 1581, 1596, 1643
signaling-groups 205, 247, 295, 334, 370, 396, 1121, 1170, 1208, 1247, 1289, 1326, 1481, 1515, 1548, 1594, 1640
simplex CM main/survivable template 214
simplex main/survivable core template 133, 256, 379
simplex main/survivable template 37, 176
simplex S8510 Server 461
simplex survivable remote template ...419, 461, 490, 575
simplex to duplex upgrade 1679
simplex to duplex upgrade template 1679
SIP Enablement Services 28
SNMP Agents 430, 1372, 1397, 1459
SNMP Traps 430, 1372, 1397, 1459
software release ...150, 260, 345, 494, 552, 670, 712, 781, 836, 847, 889, 899, 961, 971, 1015, 1025, 1133, 1150, 1182, 1302, 1360, 1379, 1445, 1569
Special 28
circumstances 28
Special circumstances 28
stage server 777
start a 137, 611, 755, 1136, 1222, 1618
SAT session on active server 137, 611, 755, 1136, 1222, 1618
starting . .42, 57, 68, 109, 124, 170, 182, 207, 219, 250, 263, 297, 309, 336, 347, 373, 398, 432, 441, 457, 466, 486, 496, 519, 529, 545, 554, 570, 585, 647, 671, 689, 713, 731, 797, 813, 821, 839, 866, 891, 963,

1016, 1041, 1073, 1093, 1122, 1173, 1185, 1210, 1250, 1263, 1293, 1303, 1329, 1349, 1374, 1382, 1399, 1417, 1437, 1446, 1460, 1483, 1516, 1550, 1572, 1598, 1607, 1643, 1653
SAT session ..42, 57, 68, 109, 124, 170, 207, 250, 297, 336, 373, 398, 432, 457, 486, 519, 545, 570, 585, 647, 689, 731, 821, 866, 1041, 1093, 1122, 1173, 1210, 1250, 1293, 1329, 1349, 1374, 1399, 1417, 1437, 1460, 1483, 1516, 1550, 1598, 1607, 1643, 1653
SAT session on active server 182, 219, 263, 309, 347, 441, 466, 496, 529, 554, 671, 713, 797, 813, 839, 891, 963, 1016, 1073, 1185, 1263, 1303, 1382, 1446, 1572
Starting Communication Manager Messaging ..201, 243, 290, 329, 366, 393, 1118, 1166, 1203, 1243, 1285, 1322, 1478, 1512, 1545, 1589, 1636
static IP address ..384, 579, 1063, 1469, 1502, 1535, 1597, 1642
Submitting 433, 1375, 1400, 1461
scheduled backups 433, 1375, 1400, 1461
super-user login 153, 627, 784, 1154
support 20
contact 20
Supported USB DVD/CD-ROM drives 1357
survivable servers 24
switch link ..207, 249, 296, 335, 372, 397, 1122, 1172, 1209, 1249, 1291, 1327, 1482, 1516, 1549, 1595, 1641
System Platform 21
System Platform Web Console 44, 59, 70, 77, 88, 98, 103, 112, 127, 163, 195, 238, 285, 324, 360, 387, 426, 450, 480, 513, 539, 564, 582, 637, 654, 680, 695, 722, 737, 806, 857, 872, 917, 938, 979, 991, 1032, 1047, 1066, 1110, 1160, 1198, 1235, 1277, 1316, 1344, 1367, 1391, 1410, 1430, 1453, 1472, 1506, 1539, 1583, 1630
accessing ...44, 59, 70, 77, 88, 98, 103, 112, 127, 163, 195, 238, 285, 324, 360, 387, 426, 450, 480, 513, 539, 564, 582, 637, 654, 680, 695, 722, 737, 806, 857, 872, 917, 938, 979, 991, 1032, 1047, 1066, 1110, 1160, 1198, 1235, 1277, 1316, 1344, 1367, 1391, 1410, 1430, 1453, 1472, 1506, 1539, 1583, 1630

T

tasks on active server 986
tasks on existing server 1038
tasks on S8510 728
tasks on S8700 .....686, 864, 924
Testing 57, 125, 171, 208, 251, 298, 336, 374, 411, 433, 457, 520, 545, 571, 600, 647, 690, 732, 813, 822, 867, 1042, 1074, 1093, 1125, 1174, 1211, 1251, 1294, 1329, 1351, 1375, 1399, 1418, 1438, 1461, 1493, 1526, 1560, 1608, 1654
the system using SAT commands ..57, 125, 171, 208, 251, 298, 336, 374, 411, 433, 457, 520, 545, 571, 600, 647, 690, 732, 813, 822, 867, 1042, 1074, 1093, 1125, 1174, 1211, 1251, 1294, 1329, 1351, 1375, 1399, 1418, 1438, 1461, 1493, 1526, 1560, 1608, 1654
The converted configuration 1698
The starting configuration 1698
third-party certificates 27
time 1150
time zone 1150
to check media modules . .171, 251, 648, 822, 1093, 1174, 1211, 1251, 1294, 1329, 1608, 1654
to resolve alarms . .174, 253, 433, 650, 663, 825, 830, 954, 1007, 1096, 1100, 1176, 1213, 1252, 1295, 1332, 1375, 1400, 1418, 1438, 1462, 1609, 1656
training 19
Transferring 147, 159, 621, 633, 764, 775, 802
files using FTP 147, 159, 621, 633, 764, 775, 802
to the services laptop computer ...147, 621, 764, 775
to the services portable computer 159, 633, 802
Transferring files to the services laptop computer ...147, 621, 764, 775
Transferring files to the services portable computer 159, 633, 802
Transferring files using FTP 147, 159, 621, 633, 764, 775, 802
translations 44, 58, 70, 97, 111, 126, 172, 208, 251, 299, 312, 337, 349, 374, 383, 412, 443, 458, 467, 497, 531, 546, 557, 578, 648, 672, 690, 715, 732, 756, 798, 823, 841, 867, 893, 948, 966, 1000, 1017, 1043, 1062, 1094, 1105, 1126, 1136, 1175, 1186, 1212, 1223, 1252, 1295, 1305, 1330, 1339, 1383, 1446, 1468, 1501, 1534, 1573, 1609, 1619, 1655
turning off 1256, 1421, 1519, 1553, 1596, 1646
the power to the control cabinet 1256, 1421, 1519, 1553, 1596, 1646
Turning off the power to the control cabinet . .1256, 1421, 1519, 1553, 1596, 1646
Turning on 778
the server 778
turning on the server 161, 635
Turning on the server 778

U

uEFI settings 283, 511, 915, 936
Updating 282, 283, 510, 511, 914, 915, 935, 936

S8800 server firmware 282, 510, 914, 935
uEFI settings of S8800 .....283, 511, 915, 936
upgrade 51, 80, 90, 119, 750, 1180, 1217, 1257, 1402, 1421, 1565, 1613
Communication Manager 51, 80, 90, 119
paths 1180
S8300 Server 1565
S8400 Server 1217, 1402, 1613
S8500 Server 1257, 1421
S8700 Server 750
sequence 1180
System Platform 51, 80, 90, 119
Upgrade Communication Manager 54, 82, 93, 121
upgrade order 30
upgrade paths 27, 1180
upgrade prerequisites for Communication Manager 1661, 1667
upgrade process 30
upgrade S8300 Server in port network 1565
upgrade S8400 Server in port network 1613
upgrade S8400 Server to S8300D Server 1217, 1402
upgrade S8500 Server to S8300D Server 1257, 1421
upgrade sequence 1180
upgrade worksheet 1667
upgrades overview 20
upgrading 1709
firmware on the new circuit packs 1709
Upgrading 51, 54, 80, 82, 91, 93, 119, 121, 461
Communication Manager template ...54, 82, 93, 121
S8510 Server to the simplex survivable remote template 461
System Platform 51, 80, 91, 119
upgrading an S8300 Server to 1179, 1377
embedded main template 1179
embedded survivable remote template 1377
upgrading an S8300 Server to embedded main template 1179
upgrading an S8300 Server to embedded survivable remote template 1377
upgrading an S8300A server to 1357
embedded survivable remote template 1357
upgrading an S8300A Server to 1131
embedded main template 1131
upgrading an S8300A Server to embedded main embedded template 1131
upgrading an S8300A server to embedded survivable remote template 1357
upgrading an S8300D server to 1299, 1441
embedded main template 1299
embedded survivable remote template 1441
upgrading an S8300D server to embedded main template 1299
upgrading an S8300D server to embedded survivable remote template 1441
Upgrading branch gateways and survivable servers 39, 65, 178, 215, 259, 306, 343, 438, 463, 526, 550, 607, 667, 709, 835, 887, 959, 1011, 1260, 1424
Upgrading DEFINITY R 1059
Upgrading DEFINITY SI 379, 575, 1103, 1337
upgrading firmware 402, 591, 1082, 1487, 1521, 1556, 1603, 1648, 1709
Upgrading firmware on the new circuit packs 1709
Upgrading System Platform 51, 80, 91, 119
Upgrading the S8510 Server to the simplex CM main/survivable core template 214
upgrading to 435, 524, 665, 707, 749, 832, 1010
duplex CM main/survivable template 665
duplex main/survivable core template 707, 832, 1010
duplex main/survivable template 749
simplex survivable remote template 435, 524
upgrading to duplex CM main/survivable template ...665
upgrading to duplex main/survivable core template . 832
upgrading to duplex main/survivable template ...63, 605, 707, 749, 884, 958
upgrading to duplex template 1010
upgrading to embedded main template 105
upgrading to simplex main/survivable core template 256
upgrading to simplex main/survivable template ..37, 133, 176
upgrading to simplex survivable remote template ...419, 435, 490, 524
USB CD/DVD reader 1195, 1314, 1364, 1389, 1452
USB flashcard drive 1195, 1364, 1389
using the book 35

V

verify ...84, 94, 169, 173, 209, 252, 299, 337, 375, 401, 458, 487, 520, 546, 571, 590, 624, 646, 649, 662, 688, 691, 702, 703, 730, 733, 744, 745, 791, 794, 821, 824, 827, 829, 865, 868, 879, 880, 923, 945, 949, 953, 985, 997, 1001, 1006, 1040, 1043, 1054, 1055, 1081, 1092, 1095, 1098, 1175, 1212, 1331, 1486, 1520, 1555, 1602, 1647, 1707
destination for scheduled backups 173, 209, 252, 299, 337, 375, 458, 487, 520, 546, 571, 649, 662, 691, 703, 733, 745, 824, 829, 868, 880, 949, 953, 1001, 1006, 1043, 1055, 1095, 1175, 1212, 1331

IPSI connectivity 84, 94, 169, 401, 590, 646, 688, 702, 730, 744, 821, 827, 865, 879, 923, 945, 985, 997, 1040, 1054, 1081, 1092, 1098, 1486, 1520, 1555, 1602, 1647, 1707
system status 791, 794
verify IPSI connectivity 84, 94, 169, 401, 590, 646, 688, 702, 730, 744, 821, 827, 865, 879, 923, 945, 985, 997, 1040, 1054, 1081, 1092, 1098, 1486, 1520, 1555, 1602, 1647, 1707
verifying ...61, 129, 150, 212, 254, 260, 302, 340, 345, 378, 384, 411, 415, 494, 552, 579, 600, 660, 670, 712, 781, 795, 814, 836, 847, 889, 899, 961, 971, 1015, 1025, 1063, 1075, 1106, 1126, 1129, 1133, 1150, 1178, 1182, 1215, 1220, 1254, 1297, 1302, 1333, 1340, 1352, 1360, 1379, 1406, 1445, 1469, 1493, 1496, 1502, 1526, 1529, 1536, 1560, 1564, 1569, 1611, 1616, 1657
Communication Manager Messaging test data ...61, 129, 212, 254, 302, 340, 378, 415, 1129, 1178, 1215, 1254, 1297, 1333, 1496, 1529, 1564, 1611, 1657
connection for server duplication 660, 795, 814, 1075
current software release 150, 260, 345, 494, 552, 670, 712, 781, 836, 847, 889, 899, 961, 971, 1015, 1025, 1133, 1150, 1182, 1302, 1360, 1379, 1445, 1569
system status ...384, 411, 579, 600, 1063, 1106, 1126, 1220, 1340, 1352, 1406, 1469, 1493, 1502, 1526, 1536, 1560, 1616
Verifying 51, 79, 89, 118, 164, 197, 239, 287, 325, 363, 388, 400, 402, 428, 452, 481, 514, 540, 565, 584, 588, 591, 638, 655, 681, 696, 723, 738, 783, 807, 858, 873, 918, 941, 980, 992, 1033, 1049, 1068, 1080, 1082, 1111, 1162, 1199, 1236, 1278, 1317, 1345, 1368, 1393, 1411, 1431, 1454, 1473, 1485, 1487, 1507, 1519, 1521, 1540, 1553, 1555, 1585, 1601, 1603, 1631, 1646, 1648, 1702, 1706
firmware version 402, 591, 1082, 1487, 1521, 1555, 1603, 1648
IPSI translations 1706
the installation of the circuit pack 400, 588, 1080, 1485, 1519, 1553, 1601, 1646, 1702
the process status 783
the software version ...51, 79, 89, 118, 164, 197, 239, 287, 325, 363, 388, 428, 452, 481, 514, 540, 565, 584, 638, 655, 681, 696, 723, 738, 807, 858, 873, 918, 941, 980, 992, 1033, 1049, 1068, 1111, 1162, 1199, 1236, 1278, 1317, 1345, 1368, 1393, 1411, 1431, 1454, 1473, 1507, 1540, 1585, 1631
verifying connectivity 863
verifying current software release 150, 260, 345, 494, 552, 670, 712, 781, 836, 847, 889, 899, 961, 971, 1015, 1025, 1133, 1150, 1182, 1302, 1360, 1379, 1445, 1569
Verifying firmware version 402, 591, 1082, 1487, 1521, 1555, 1603, 1648
Verifying IPSI translations 1706
Verifying the connection for server duplication ..660, 795, 814, 1075
Verifying the installation of the circuit pack 400, 588, 1080, 1485, 1519, 1553, 1601, 1646, 1702
Verifying the process status 783
Verifying the software version ...51, 79, 89, 118, 164, 197, 239, 287, 325, 363, 388, 428, 452, 481, 514, 540, 565, 584, 638, 655, 681, 696, 723, 738, 807, 858, 873, 918, 941, 980, 992, 1033, 1049, 1068, 1111, 1162, 1199, 1236, 1278, 1317, 1345, 1368, 1393, 1411, 1431, 1454, 1473, 1507, 1540, 1585, 1631
videos 19
Avaya Mentor 19
view 180, 217, 261, 308, 345, 440, 465, 494, 528, 553, 669, 711, 837, 848, 889, 900, 962, 972, 1013, 1024, 1182, 1261, 1301, 1380, 1443, 1570
the configuration screens 180, 217, 261, 308, 345, 440, 465, 494, 528, 553, 669, 711, 837, 848, 889, 900, 962, 972, 1013, 1024, 1182, 1261, 1301, 1380, 1443, 1570
Viewing 135, 421, 609, 753, 767, 1134, 1360
the configuration screens to copy or print ...135, 421, 609, 753, 767, 1134, 1360

W

warranty 20
Web Console 44, 59, 70, 77, 88, 98, 103, 112, 127, 163, 195, 238, 285, 324, 360, 387, 426, 450, 480, 513, 539, 564, 582, 637, 654, 680, 695, 722, 737, 806, 857, 872, 917, 938, 979, 991, 1032, 1047, 1066, 1110, 1160, 1198, 1235, 1277, 1316, 1344, 1367, 1391, 1410, 1430, 1453, 1472, 1506, 1539, 1583, 1630
accessing ...44, 59, 70, 77, 88, 98, 103, 112, 127, 163, 195, 238, 285, 324, 360, 387, 426, 450, 480, 513, 539, 564, 582, 637, 654, 680, 695, 722, 737, 806, 857, 872, 917, 938, 979, 991, 1032, 1047, 1066, 1110, 1160, 1198, 1235, 1277, 1316, 1344, 1367, 1391, 1410, 1430, 1453, 1472, 1506, 1539, 1583, 1630