



Installing and Upgrading the Avaya G700 Media Gateway and Avaya S8300 Media Server

555-234-100
Issue 10.2
May 2007

© 2007 Avaya Inc.
All Rights Reserved.

Notice

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

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

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

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: <http://www.avaya.com/support>.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

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

Contents

About this book	27
Overview	27
Audience	27
Using this book	27
Conventions	29
Physical dimensions	29
Terminology	30
Typography	30
Commands	31
Keys.	31
User input	32
System output and field names.	32
Downloading this book	32
Safety labels and security alert labels	33
Related resources	33
Technical assistance	34
Within the United States.	34
International	35
Trademarks.	35
Ordering Documentation	35
Sending us comments.	36
 Section 1: Reference information and hardware installation	 37
 Chapter 1: Roadmaps and reference information	 39
What wizards are available	39
Where are the most recent versions of the Wizards	40
When to use each wizard	40
About connection and login methods	41
What physical access methods are available	41
Laptop configuration for direct connection to the services port.	42
What network settings are required on the laptop	43
Configuring the laptop for a direct connection	43
About connection methods	48
Connecting a laptop to services port of S8300	48
Connecting a laptop to the G700 serial port	48
Connecting a laptop to the customer LAN.	49
Connecting an external modem to the S8300 media server	49

Contents

Setting up Windows for modem connection to the media server (Windows 2000 or XP)	50
Configuring the Remote PC for PPP Modem Connection (Windows 2000 or XP, Terminal Emulator, or ASA)	51
Using Windows for PPP Modem Connection (Windows 2000 or XP)	52
Using Avaya Terminal Emulator for LAN Connection to Communication Manager	53
Using Avaya Terminal Emulator for Modem Connection to Communication Manager	54
About Log in Methods	55
Accessing the server's command line interface with SSH	55
Logging in to the media server from your laptop using Telnet.	56
Logging in to the S8300 Web Interface from your laptop	57
Open the Communication Manager SAT Screens	62
Logging in to the P330 Stack Processor with a Direct Connection to the S8300 Services Port	62
Logging in to the P330 Stack Processor with a LAN Connection	63
Logging in to the P330 Stack Processor with a Direct Serial Connection	64
Logging in to the P330 Stack Processor with Device Manager.	64
About Avaya Site Administration	65
Configuring Avaya Site Administration	65
About navigation for G700 CLI commands	67
About terminal emulation function keys for Communication Manager	68
 Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server.	 69
About hardware components	69
What are the main elements of the G700 media gateway	69
What comprises the G700 media gateway chassis and processors	70
What are the media modules	70
What are data expansion modules	72
What are stackable ethernet switches	73
Building a stack	75
What are the functions of the S8300 LED Indicators	78
Media servers supporting the G700 media gateway	79
What is the S8300 media server	79
What is the S8400 media server	80
What is the S8500 media server	80
What is the S8700/S8710/S8720 media server	80
About endpoint and adjunct components	81

About installation planning	81
What the planning documentation provides	82
Who needs a Single Sign-On (SSO) authentication login	82
What site verification does	83
What network integration requires	83
Reviewing demarcation points and connectivity for the IA770 INTUITY AUDIX Messaging Application.	83
Maintaining system security	84
Verifying features for the IA770 INTUITY AUDIX Messaging Application .	84
About installation and cabling	85
Verifying the on-site checklist	85
Verifying Environmental conditions	86
Power Verification	86
Grounding Verification	86
Unpacking and checking the order.	87
Installing the G700 media gateway	87
Preparing the G700 media gateway.	88
Mounting the G700 media gateway in the rack	89
Inserting the Avaya S8300 media server (if necessary for standalone service or LSP).	91
Inserting media modules	93
Inserting an Expansion Module.	96
Inserting an Avaya X330STK Stacking Module	97
Cabling multiple units	98
Attaching Ground Conductors	102
What are general grounding requirements.	102
What are approved grounds	103
Connecting the Safety Ground	105
Connecting AC Power	106
What are the G700 AC power requirements	106
Testing the AC Outlet	106
Plugging in AC power	108
Checking and Connecting DC Power	109
Section 2: G700 installation and upgrades - wizards	111
About the Installation Roadmap and Task Lists	112
Chapter 3: Installing a new G700 with an S8300 using the Avaya Installation Wizard	113
Installation Overview	114
About software and firmware files	114

Contents

About access to the Communication Manager software distribution CD . . .	114
Tasks to install the S8300 and G700	114
Before Going to the Customer Site.	116
Obtaining a USB DVD or CD-ROM drive	116
Getting information that the project manager provides.	116
Electronic pre-installation worksheet	116
Name and number list	116
Custom template.	117
Getting the Serial Number of the G700, if Necessary.	117
Checking for and FTP/SCP/SFTP Server or Compact Flash for Backing up Data	118
Obtaining service pack files, if needed.	118
Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary	119
Obtaining an IA770 service pack file	119
Obtaining Optional language files	120
Obtaining Ethernet interface IP address and subnet mask.	120
Completing the RFA process (Obtaining license and password file)	120
Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary	122
Install the S8300	123
Inserting the S8300	123
Installing Communication Manager Software	124
Setting telnet parameters	124
Remastering the hard drive and installing the software	125
Accessing the S8300	128
Creating a super-user login, if necessary, for R4.0 or higher	129
Using the Avaya Installation Wizard (IW).	133
Telephony configuration	151
Trunk configuration	155
Adding a trunk	157
Modifying trunk parameters.	158
Modifying IP route configuration	159
Displaying trunk status	160
Removing a trunk	161
Configuring a trunk media module	162
Endpoint installation	163
Alarm configuration	164
Password and final screens.	166

If the server is an LSP, stop and start Communication Manager.	171
Configuring an X330 Expansion Module (if necessary)	172
Setting rapid spanning tree on the network	173
Administering an S8300 primary controller	174
Assigning Node Names and IP Addresses for the LSPs	175
Administering Network Regions	175
Associating LSPs with Network Regions	176
Administering IP Interfaces	177
Identifying LSPs to the S8300 primary controller	178
Administering an S8400, S8500, or S8700-series primary controller	179
Assigning Node Names and IP Addresses for the C-LANs and LSPs	180
Administering Network Regions	181
Assigning LSPs to the Network Regions	183
Administering IP Interfaces	184
Identifying the Survivable Processor on the primary controller	188
Administering the Media Gateway	189
Saving Communication Manager translations.	192
Considerations for IP Phones Supported by a Local Survivable Processor	193
Transition of Control from Primary Controller to LSP	194
Complete the Installation of the S8300 (if the Primary Controller)	195
Updating IA770 INTUITY AUDIX Messaging, if installed	195
Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update. .	195
Installing IA770 service pack (or RFU) files, if any	196
Starting IA770 INTUITY AUDIX Messaging	196
Verifying start up of IA770 INTUITY AUDIX Messaging	197
If IA 770 fails to start after a new installation	198
Saving translations	198
Backing up the system	198
If using IA770, administer Communication Manager for Integrated Messaging. .	200
Complete the Installation Process (for an S8300 LSP)	200
 Chapter 4: Installing a new G700 without an S8300 using the Gateway Installation Wizard	 201
Installation overview.	202
What are the system components	202
About G700 components	202
About firmware files	202
About the TFTP server.	202

Contents

What provides initial access to the G700	202
Before going to the customer site	203
Getting information that the project manager provides.	203
Installing the Gateway Installation Wizard	203
Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary.	203
Downloading G700 firmware files to your TFTP directory	204
Downloading individual firmware files	204
Configure the G700 and upgrade firmware	206
Connecting to the G700 console port	206
Configure an X330 Expansion Module (If Necessary)	220
Set rapid spanning tree on the network	221
Administer Communication Manager	222
Administering an S8300 primary controller	222
Assigning Node Names and IP Addresses for the LSPs	223
Administering Network Regions	223
Associating LSPs with Network Regions	224
Administering IP Interfaces	225
Identifying LSPs to the S8300 primary controller	226
Administering an S8400, S8500, or S8700-series primary controller	227
Assigning Node Names and IP Addresses for the C-LANs and LSPs	228
Administering Network Regions	229
Assigning LSPs to the Network Regions.	231
Administering IP Interfaces	232
Identifying the Survivable Processor on the primary controller	236
Administering the Media Gateway	237
Complete the Installation Process	240
Chapter 5: Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool	241
Considerations for upgrading the S8300B as a primary controller or as an LSP	242
Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323	243
The need to restore IP Phone files	243
Major tasks to upgrade the S8300B to release 4.0 and upgrade the G700 firmware.	244
Before going to the customer site	244
Obtaining a USB DVD/CD-ROM drive.	245
Getting information that the project manager provides.	245
Getting the serial number of the G700, if necessary	245
Checking the number of allocated ports	245

Checking the versions of the LSPs (if starting from R2.0 only)	246
Checking for and FTP/SCP/SFTP Server or Compact Flash for Backing up Data	246
Obtaining S8300 software and G700 firmware.	246
Checking the CD for the most recent files	247
Obtaining service pack files	247
Pre-upgrade service pack (starting from R2.x only).	247
Post-upgrade service pack	248
Obtaining service pack and language files for IA770 INTUITY	
AUDIX Messaging, if necessary	249
Checking for IA770 stored messages size	249
Obtaining an IA770 service pack file	250
Obtaining optional language files	250
Completing the RFA process (obtaining license and password file).	250
Ensuring a super-user login exists.	252
Checking a pre-4.0 release	253
Checking a 4.0 release.	253
Creating a super-user login, if one does not exist (releases earlier than Release 4.0)	254
Creating a super-user login, if necessary, for R4.0 or higher	255
On-site Preparation for the Upgrade	258
Setting up a TFTP server or HTTP server for LSP software download, if desired	259
Accessing the S8300	260
Removing the administration for the IA770 integration if CWY1 board is used	260
Completing pre-upgrade tasks — If the target S8300 is the primary controller	261
Saving a copy of the 4600-series phone configuration file, if any	264
Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used)	265
Determining whether optional languages are needed.	265
Downloading optional language files, if needed.	267
Creating an IA770 test message for the upgrade	268
Shutting down IA770.	268
Backing up S8300 recovery system files.	269
Copying the service pack files to the media server (starting from R2.x only).	272
Installing the pre-upgrade software service pack (starting from R2.x only).	272
Copying Files to the S8300 hard drive	273
Copying authentication files to the LSPs	275
Copying the Communication Manager software and media gateway firmware to a TFTP or HTTP server	275

Contents

Copying the Communication Manager software and media gateway firmware to the server	275
Preparing LSPs	275
Obtaining additional data for running the Upgrade Tool	280
Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways	281
Checking the current releases of all devices (optional).	281
Running the upgrade	284
Viewing the status of the upgrade in progress	286
Creating a customer login, if necessary	287
Installing updated authentication files	290
If upgrading an LSP, synchronize translations from the primary controller.	290
If the server is an LSP, stop and start Communication Manager.	291
Saving translations	291
Ensuring the MGP default gateway IP address is set	291
Setting rapid spanning tree on the network	293
Post-upgrade tasks	294
Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update.	294
Installing IA770 service pack (or RFU) files, if any	294
Starting IA770 INTUITY AUDIX Messaging.	295
Verifying start up of IA770 INTUITY AUDIX Messaging	295
Saving translations	296
If using IA770, administering switch integration for H.323	297
Testing to verify system functionality	297
Copying IP Phone firmware to the media server, if necessary	297
Restoring the 4600-series phone configuration file, if any	298
Completing the upgrade process (S8300 is the primary controller)	298
 Chapter 6: Upgrading an existing G700 without an S8300 using the Upgrade Tool	 301
About the existing G700 upgrade.	301
What are the G700 system components	301
About firmware files	302
About the TFTP server.	302
About system access	302
Accessing the G700	302
Before going to the customer site	303
Planning forms that the project manager provides	303
Setting up the TFTP server on your laptop or on a customer PC, if necessary	303

Downloading G700 firmware files to your TFTP directory	304
Downloading individual firmware files	304
On-site preparation for the upgrade	306
Accessing the P330 Stack Processor	306
Verifying the contents of the tftpboot directory	306
Determining which firmware to install on the G700	307
Running the upgrade	311
Ensuring the MGP default gateway IP address is set	313
Setting rapid spanning tree on the network	314
Chapter 7: Telephones and adjunct systems	315
Installation and wiring of telephones and power supplies	316
About connectable telephones and consoles	316
Connecting telephones	317
Connecting an analog station or 2-wire digital station	317
Connecting an ISDN BRI station to an MM720 Media Module	318
Installing an 808A Emergency Transfer Panel and associated telephones	319
Installing and wiring telephone power supplies	321
Typical adjunct power connections	321
Typical adjunct power connections end-to-end	322
Auxiliary power for an attendant console	323
1152A1 mid-span power distribution units.	324
Connecting the 1152A1 PDU cables	326
1152B mid-span power distribution units	329
Connecting the 1152B PDU cables	331
1151B1/C1 and 1151B2/C2 power supplies	333
Important safety instructions for 1151B1/C1 and 1151B2/C2 power supplies	334
Using the 1151B1/C1 and 1151B2/C2 power supplies.	334
Connecting the 1151B1/C1 or 1151B2/C2 power supplies	335
C360-PWR Power over Ethernet converged stackable switches.	336
Important C360T-PWR switch safety instructions.	336
UL safety standards compliance	337
Compatibility	338
Power Specifications	338
Using the C360T-PWR switches	338
Connecting the C360T-PWR switches	338
Connecting the cables.	339
Additional information.	339

Contents

Complete the telephone installation process	340
Installing the coupled bonding conductor	340
Installing over-voltage and sneak-current circuit protection	341
IA 770 INTUITY AUDIX messaging application	342
Shared resources of IA770 coresidency	342
Where is the IA770 location and software	343
Using an AUDIX trunk group as well as an AUDIX hunt group for new systems	343
IA 770 INTUITY AUDIX installations and S8300 upgrades for IA 770 INTUITY AUDIX	343
INTUITY AUDIX LX messaging system	344
ASAI co-resident DEFINITY LAN gateway (DLG)	344
PROCR administration task summary (for the S8300 Media Server)	345
Supported Ethernet Interfaces	346
Call center	346
About Avaya G700 announcement software	347
Avaya Integrated Management	349
Avaya ATM WAN Survivable Processor Manager	349
Avaya Directory Enabled Management	350
Avaya Network Management Console with VoIP SystemView	350
Avaya MultiService SMON Manager	351
Avaya Fault and Performance Manager	351
Avaya Proxy Agent	351
Avaya Configuration Manager	351
Avaya Site Administration	352
Avaya Terminal Configuration	352
Avaya Terminal Emulator	352
Avaya Voice Announcement Over LAN Manager	353
Avaya VoIP Monitoring Manager	353
Uninterruptible power supply (UPS)	354
Terminal server installation	356
Installing and administering the terminal server	356
What are the distance limits for the terminal server.	357
How is the terminal server cabling connected.	358
Connecting the IOLAN+ to the adjunct and the LAN	358
Administering the IOLAN+	359
Navigating the IOLAN+ terminal server	363
Administering the gateway	364

Administering an IOLAN+ port	364
Testing connectivity through the IOLAN+	366
Potential failure scenarios and repair actions	368
Administering IP services	368
Call detail recording (CDR)	370
Connecting CDR equipment	370
Administering CDR data collection	370
Administering CDR parameters	371
Testing the switch-to-adjunct link	373
Reliable Data Transport Tool (RDTT) package	374
What does the RDTT package contain	374
Downloading the RDTT package	374
Installing the RDTT package	375
Administering the RDTT package	375
Related topics	375
Printers	375
DS1/T1 CPE loopback jack	376
Installing a loopback jack	376
Installing a loopback jack with a smart jack	376
Installing a loopback jack without a smart jack	377
Administering a loopback jack	378
Testing a loopback jack with a smart jack	378
Testing the DS1 span from the ICSU to the loopback jack	378
Checking the integrity of local equipment	379
Testing the integrity of data sent over the loop	380
Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer (MUX)	383
Testing the DS1 span from the loopback jack to the smart jack	383
Testing a loopback jack without a smart jack	387
Configurations using fiber multiplexers	390
Checking for the presence of DC	390
External modems	391
Hardware required when configuring modems	391
Multi-Tech MT5634ZBA-USB-V92	391
Configuring the MT5634ZBA-USB-V92 modem	392
Multi-Tech MT5634ZBA-V92-GLOBAL	392
Administering Multi-Tech modems	392
Busy tone disconnect equipment for non-U.S. installations	393

Contents

Music-on-hold	394
Installing an unregistered music source on a G700 or G350 Media Gateway	394
Installing a registered music source on a G700 or G350 Media Gateway	397
Paging and announcement equipment	398
Adjunct Information Sources	399
Call Management System	399
INTUITY AUDIX Messaging Systems	400
Avaya Modular Messaging System	400
ASAI and DEFINITY LAN Gateway	400
Avaya Interactive Response	400
Avaya EC500 Extension to Cellular and Off-PBX Stations	401
SIP Enablement Services	401
Seamless Converged Communications across Networks (SCCAN)	401
Call Accounting Systems	401
 Section 3: G700 installation and upgrades - manual procedures.	 403
 Chapter 8: Manual installation of a new G700 with an S8300	 405
Installation Overview	406
About software and firmware files	406
About access to the Communication Manager software distribution CD	406
Tasks to install the S8300 and the G700	406
Before Going to the Customer Site.	408
Obtaining a USB DVD or CD-ROM drive	409
Getting information that the project manager provides.	409
Getting the serial Number of the G700, if necessary	409
Checking for and FTP/SCP/SFTP server or compact flash for backing up data	409
Obtaining service pack files, if needed.	410
Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary	411
Obtaining an IA770 service pack file	411
Obtaining Optional language files	412
Obtaining Ethernet interface IP address and subnet mask.	412
Completing the RFA process (Obtaining license and password file)	412
Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary	413
Install the S8300	415
Inserting the S8300	415

Installing Communication Manager Software	416
Setting telnet parameters	416
Remastering the hard drive and installing the software	417
Accessing the S8300	420
Verifying Software Version	420
Copying Files to the S8300 hard drive	421
Downloading optional language files, if needed.	423
Verifying the Time, Date, and Time Zone.	423
Creating a super-user login, if necessary, for R4.0 or higher	424
If upgrading an LSP, synchronize translations from the primary controller.	427
Configuring the S8300.	428
Providing the keys.install File (If Necessary)	440
Installing the license and authentication files	441
If the server is an LSP, stop and start Communication Manager.	443
Installing security files and Communication Manager service packs, if any	443
Saving Translations	445
Configure the G700 Media Gateway	446
Assigning IP Addresses of the G700 Media Gateway Components	446
Checking for IP connections	451
Setting up the Controller List for the G700	452
Setting the LSP Transition Points	454
Configuring an X330 Expansion Module (If Necessary)	455
Install New Firmware on the G700	455
Manual upgrade procedures — G700 firmware	455
Verifying the Contents of the tftpboot Directory.	456
Determining which firmware to install on the G700	456
Installing New Firmware on the P330 Stack Processor	458
Installing new firmware on the G700 Media Gateway Processor.	459
Installing new firmware on the media modules	461
Setting rapid spanning tree on the network	463
Administer Communication Manager	464
Administering an S8300 primary controller	464
Assigning Node Names and IP Addresses for the LSPs	465
Administering Network Regions	466
Associating LSPs with Network Regions	467
Administering IP Interfaces	468
Identifying LSPs to the S8300 primary controller	469
Administering an S8400, S8500, or S8700-series primary controller	470
Assigning Node Names and IP Addresses for the C-LANs and LSPs	471
Administering Network Regions	472

Assigning LSPs to the Network Regions.	474
Administering IP Interfaces	475
Identifying the Survivable Processor on the primary controller	479
Administering the Media Gateway	480
Considerations for IP Phones Supported by a Local Survivable Processor	484
Transition of Control from Primary Controller to LSP	485
Set Up SNMP Alarming on the G700	485
Configuring the primary server to report alarms to a services support agency	486
Administering INADS phone numbers and Enabling alarms to INADS . .	486
Configuring the G700 Media Gateway to send its traps	
to a network management system (NMS).	487
Configuring an SNMP community string for traps	487
Configuring the destination for G700 SNMP traps	488
Complete the Installation of the S8300	
(if the Primary Controller)	489
Updating IA770 INTUITY AUDIX Messaging, if installed	489
Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update. .	489
Installing IA770 service pack (or RFU) files, if any	490
Starting IA770 INTUITY AUDIX Messaging	490
Verifying start up of IA770 INTUITY AUDIX Messaging	491
If IA 770 fails to start after a new installation	492
Saving translations	492
Backing up the system	492
If using IA770, administer Communication Manager for Integrated Messaging. .	494
If IA 770 fails to start after a new installation	494
Complete the Installation Process	
(for an S8300 LSP)	494
Chapter 9: Manual installation of a new G700 without an S8300	495
Installation overview.	497
What are the system components	497
About G700 components	497
About firmware files	497
About the TFTP server.	497
What provides initial access to the G700	497
Before going to the customer site	498
Getting information that the project manager provides.	498
Setting Up the TFTP Server on Your Laptop or	
on a Customer PC, if Necessary.	498
Downloading G700 firmware files to your TFTP directory	498

Downloading individual firmware files	499
Configure the G700	500
Assigning the IP addresses of the G700 media gateway components	501
Checking for IP connections	505
Setting up the controller list for the G700	506
Setting the LSP Transition Points	509
Configuring an X330 Expansion Module (If Necessary)	509
Prepare to install firmware on the G700	510
Accessing the P330 Stack Processor	510
Verifying the contents of the tftpboot directory	510
Determining which firmware to install on the G700	511
Install new firmware on the G700 Media Gateway	513
Installing new firmware on the P330 stack processor.	513
Installing new firmware on the G700 Media Gateway Processor	514
Installing new firmware on the media modules	515
Setting rapid spanning tree on the network	517
Administer Communication Manager	518
Administering an S8300 primary controller	519
Assigning Node Names and IP Addresses for the LSPs	519
Administering Network Regions	520
Associating LSPs with Network Regions	521
Administering IP Interfaces	522
Identifying the Survivable Processor on the primary controller	523
Administering an S8400, S8500, or S8700-series primary controller	524
Assigning Node Names and IP Addresses for the C-LANs and LSPs	525
Administering Network Regions	526
Assigning LSPs to the Network Regions.	528
Administering IP Interfaces	529
Identifying the Survivable Processor on the primary controller	533
Administering the Media Gateway	534
Complete the Installation Process	538
Chapter 10: Manual upgrade of an S8300A and G700 to R4.0	539
About upgrading an S8300A to R4.0	539
Issues for IA770 INTUITY AUDIX on Release 1.3 or earlier on an S8300A Media Server.	540
Tasks to upgrade the S8300A to release 4.0 and upgrade the G700 firmware	541
Before going to the customer site	543
Obtaining a USB DVD/CD-ROM drive.	544

Getting information that the project manager provides.	544
Filling in the EPW, if upgrading from release 1.3 or earlier.	544
Getting the serial number of the G700, if necessary	544
Checking the number of allocated ports	545
Checking the availability of the FTP server for backing up data	545
Obtaining S8300 software and G700 firmware.	545
Obtaining service pack files, if needed.	546
Obtaining service pack and language files for IA770 INTUITY	
AUDIX Messaging, if necessary	548
Checking the size of stored messages (CM 2.0 only)	548
Obtaining an IA770 service pack file	548
Obtaining optional language files	549
Completing the RFA process	
(obtaining license and password files)	549
Downloading license file and password for an LSP.	549
Running the Automatic Registration Tool (ART)	
for the INADS IP address, if necessary	550
Ensuring a super-user login exists.	551
Checking a pre-4.0 release	552
Creating a super-user login, if one does not exist (releases earlier than Release 4.0)	553
Preparing for the upgrade to R4.0 on-site	555
Accessing the S8300	555
Removing the administration for the IA770 integration if CWY1 board is used	555
Checking current software release.	556
Completing pre-upgrade tasks — if the S8300 is the primary controller . . .	557
Getting IA770 data and stopping IA770	
(if IA770 is being used).	561
Creating an IA770 test message (R2.0 only)	561
Determining whether optional languages are needed.	561
Checking for any IA770 custom announcement sets (R2.0 only)	563
Stopping IA770.	564
Backing up system files.	565
Recording configuration information	568
Replacing the S8300A	569
Installing the pre-upgrade software service pack, if necessary	569
Installing the pre-upgrade service pack	570
Linux migration backup	
(if current release is 1.2.0 through 1.3.x)	572
Replacing the S8300A with the S8300B or S8300C Media Server	575

Upgrading the S8300B or S8300C Media Server.	577
Setting telnet parameters	577
Remastering the S8300 and installing the upgrade software.	577
Verifying software version	581
Copying Files to the S8300 hard drive	581
Downloading optional language files, if needed.	583
Installing security and Communication Manager service pack updates, if any	583
Setting the Time, Date, and Time Zone.	585
Configuring network parameters	585
Verifying connectivity	588
Disabling RAM disk on the media server	588
Rebooting the media server.	588
Restoring data backup	589
Checking for the IA770 IP address	592
Enabling RAM disk on the media server	593
Rebooting the media server.	593
Installing updated license and authentication files	594
Checking a 4.0 release for a super-user login	595
Creating a super-user login, if necessary, for R4.0 or higher	596
If upgrading an LSP, synchronize translations from the primary controller. .	599
If the server is an LSP, stop and start Communication Manager.	599
Verifying media server configuration (Release 1.2 or later)	600
If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started.	601
Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary.	602
Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary	602
If IA 770 fails to start after an upgrade	602
Saving translations	603
Upgrade the firmware on the G700 Media Gateway	604
Verifying the contents of the tftpboot directory	604
Determining which firmware to install on the G700	605
Installing new firmware on the P330 Stack Processor	606
Installing new firmware on the G700 Media Gateway Processor.	607
Installing new firmware on the media modules	609
Ensuring the MGP default gateway IP address is set	611
Setting rapid spanning tree on the network	611
Installing new firmware on other G700 media gateways	612
Post-upgrade tasks	613
Stopping IA770 INTUITY AUDIX Messaging, if installed	613
Installing IA770 service pack (or RFU) files, if any	614

Starting IA770 INTUITY AUDIX Messaging, if installed	614
Verifying start up of IA770 INTUITY AUDIX Messaging, if installed	615
Saving translations	616
If using IA770, administering switch integration for H.323	616
Administering IA770 (Release 1.3 or earlier).	616
Testing to verify system functionality	616
Complete the upgrade process (S8300 is the primary controller)	617
Chapter 11: Manual upgrade of an existing S8300B or S8300C and G700 to R4.0	619
Considerations for upgrading the S8300B or S8300C as a primary controller or as an LSP	619
Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323	620
The need to restore IP Phone files	621
Tasks to upgrade the S8300B or S8300C to release 4.0 and upgrade the G700 firmware.	621
Before going to the customer site	623
Obtaining a USB DVD/CD-ROM drive.	623
Getting information that the project manager provides.	623
Getting the serial number of the G700, if necessary	624
Checking the number of allocated ports	624
Checking for and FTP/SCP/SFTP Server or Compact Flash for Backing up Data	624
Obtaining S8300 software and G700 firmware.	625
Checking the CD for the most recent firmware files.	625
Obtaining service pack files	625
Pre-upgrade service pack (starting from R2.x only).	626
Post-upgrade service pack	626
Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary	627
Checking for IA770 stored messages size	628
Obtaining an IA770 service pack file	628
Obtaining optional language files	629
Completing the RFA process (obtaining license and password file).	629
Downloading license file and Communication Manager versions for an LSP	629
Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary	630
Ensuring a super-user login exists.	631
Checking a pre-4.0 release	631

Checking a 4.0 release.	632
Creating a super-user login, if one does not exist (releases earlier than Release 4.0)	633
Creating a super-user login, if necessary, for R4.0 or higher	634
On-site Preparation for the Upgrade	637
Accessing the S8300	637
Removing the administration for the IA770 integration if CWY1 board is used	638
Completing pre-upgrade tasks — if the target S8300 is the primary controller	638
Saving a copy of the 4600-series phone configuration file, if any	641
Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used)	642
Determining whether optional languages are needed.	642
Downloading optional language files, if needed.	645
Creating an IA770 test message for the upgrade	645
Shutting down IA770.	645
Backing up S8300 recovery system files.	647
Copying and installing the service pack files to the media server (starting from R2.x only)	649
Copying Files to the S8300 hard drive	650
Copying the software and firmware files to the server	652
Upgrade the S8300.	657
Installing new software	657
Installing updated authentication files	660
If upgrading an LSP, synchronize translations from the primary controller. .	662
If the server is an LSP, stop and start Communication Manager.	662
Installing security and Communication Manager service pack updates, if any	662
If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started.	664
Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary.	665
Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary	665
If IA 770 fails to start after an upgrade	665
Test to verify system functionality	666
Making the upgrade permanent.	666
Saving translations	666
Copying IP Phone firmware to the media server, if necessary	667
Restoring the 4600-series phone configuration file, if any	668
Upgrade the G700 Firmware	668
Verifying the contents of the tftpboot directory	668
Determining which firmware to install on the G700	669

Installing new firmware on the P330 stack processor.	671
Installing new firmware on the G700 Media Gateway Processor.	672
Installing new firmware on the media modules	673
Ensuring the MGP default gateway IP address is set	675
Setting rapid spanning tree on the network	676
Installing new firmware on other G700 media gateways	677
Post-upgrade tasks	678
Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update.	678
Installing IA770 service pack (or RFU) files, if any	678
Starting IA770 INTUITY AUDIX Messaging.	679
Verifying start up of IA770 INTUITY AUDIX Messaging	679
Saving translations	680
If using IA770, administering switch integration for H.323	681
Testing to verify system functionality	681
Completing the upgrade process (S8300 is the primary controller)	681
Backing up the system	683
 Chapter 12: Manual upgrade of an existing S8300B and G700 to S8300C with R4.0	 685
Considerations for upgrading the S8300B as a primary controller or as an LSP	685
Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323	686
The need to restore IP Phone files	687
Tasks to upgrade the S8300B to S8300C on release 4.0 and upgrade the G700 firmware.	687
Before going to the customer site	689
Obtaining a USB DVD/CD-ROM drive.	690
Getting information that the project manager provides.	690
Getting the serial number of the G700, if necessary	690
Checking the number of allocated ports	690
Checking the availability of the FTP, SFTP, or SCP server for backing up data	691
Obtaining S8300 software and G700 firmware.	691
Checking the CD for the most recent firmware files.	691
Obtaining service pack files, if needed.	692
Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary	693
Checking for IA770 stored messages size	693
Obtaining an IA770 service pack file	694
Obtaining optional language files	694

Completing the RFA process (obtaining license and password file).	694
Downloading license file and Communication Manager versions for an LSP	695
Running the Automatic Registration Tool (ART) for the INADS IP address, if necessary	696
Ensuring a super-user login exists.	697
Checking a pre-4.0 release	697
Checking a 4.0 release.	698
Creating a super-user login, if one does not exist (releases earlier than Release 4.0)	698
On-site Preparation for the Upgrade	700
Accessing the S8300	700
Removing the administration for the IA770 integration if CWY1 board is used	700
Completing pre-upgrade tasks — If the target S8300 is the primary controller	701
Saving a copy of the 4600-series phone configuration file, if any	704
Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used)	704
Determining whether optional languages are needed	705
Checking for any IA770 custom announcement sets	707
Creating an IA770 test message for the upgrade	707
Shutting down IA770	707
Backing up S8300 recovery system files.	708
Recording configuration information	711
Upgrade the S8300.	712
Replacing the S8300B with the S8300C Media Server	712
Remastering the hard drive and installing the software	714
Verifying Software Version	717
Copying Files to the S8300 hard drive	717
Downloading optional language files, if needed.	719
Installing security and Communication Manager service pack updates, if any	719
Setting the Time, Date, and Time Zone.	721
Configuring network parameters	721
Verifying connectivity	724
Disabling RAM disk on the media server	724
Rebooting the media server.	724
Restoring all data	725
Checking for the IA770 IP address	728
Enabling RAM disk on the media server	729
Rebooting the media server.	729
Installing updated license and authentication files	730
Checking a 4.0 release for a super-user login	731

Contents

Creating a super-user login, if necessary, for R4.0 or higher	732
If upgrading an LSP, synchronize translations from the primary controller. .	735
If the server is an LSP, stop and start Communication Manager.	736
If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started.	736
Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary.	737
Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary	737
If IA 770 fails to start after an upgrade	738
Saving translations	738
Copying IP Phone firmware to the media server, if necessary	739
Restoring the 4600-series phone configuration file, if any	740
Upgrade the G700 firmware	740
Verifying the contents of the tftpboot directory	740
Determining which firmware to install on the G700	741
Installing new firmware on the P330 stack processor.	743
Installing new firmware on the G700 Media Gateway Processor.	744
Installing new firmware on the media modules	745
Ensuring the MGP default gateway IP address is set	747
Setting rapid spanning tree on the network	748
Installing new firmware on other G700 media gateways	749
Post-upgrade tasks	750
Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update. . . .	750
Installing IA770 service pack (or RFU) files, if any	750
Starting IA770 INTUITY AUDIX Messaging.	751
Verifying start up of IA770 INTUITY AUDIX Messaging	751
Saving translations	752
If using IA770, administering switch integration for H.323	753
Testing to verify system functionality	753
Completing the upgrade process (S8300 is the primary controller)	753
Backing up the system	755
 Chapter 13: Manual upgrade of an existing G700 without an S8300 to R4.0	 757
About the existing G700 upgrade.	757
What are the G700 system components	757
About firmware files	758
About the TFTP server.	758
About system access	758
Accessing the G700	758

Before going to the customer site	759
Planning forms that the project manager provides	759
Setting up the TFTP server on your laptop or on a customer PC, if necessary	759
Downloading G700 firmware files to your TFTP directory	760
Downloading individual firmware files	760
On-site preparation for the upgrade	762
Accessing the P330 stack processor.	762
Verifying the contents of the tftpboot directory	762
Determining which firmware to install on the G700	763
Install new firmware on the G700 Media Gateway.	765
Manually installing G700 and media modules firmware	765
Installing new firmware on the P330 stack processor.	766
Installing new firmware on the G700 Media Gateway Processor	766
Installing new firmware on the media modules	768
Ensuring the MGP default gateway IP address is set	770
Setting rapid spanning tree on the network	771
Appendix A: Technical information	773
Avaya G700 Media Gateway Technical Specifications	773
Cabling Equipment	774
Appendix B: Information checklists	777
Installer's Checklist	778
Serial Number and Login Information	779
G700 Serial Numbers	779
Logins	779
Set-Up for P330 Stack Processor.	780
Set Up for G700 Media Gateway Processor (MGP)	781
Set Up for VoIP Resources	782
Set Up for S8300 Media Server	783
Installation Site Information.	784
Stack Layout	785
Appendix C: Equipment list.	787
Appendix D: Install the Avaya TFTP server	797
Index	803

About this book

Overview

This document provides procedures to install, upgrade, or add to an Avaya G700 Media Gateway controlled by an Avaya S8300, S8400, S8500, or S8700/S8710/S8720 Media Server. It also includes information on connecting telephones and adjuncts to the G700.

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

Audience

This book is for the following audiences:

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

Using this book

This book is organized into three major sections:

- [Section 1: Reference information and hardware installation](#)
- [Section 2: G700 installation and upgrades - wizards](#)
- [Section 3: G700 installation and upgrades - manual procedures](#)

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

- [Chapter 1: Roadmaps and reference information](#)
- [Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server](#)

About this book

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

- [Chapter 3: Installing a new G700 with an S8300 using the Avaya Installation Wizard](#)
- [Chapter 4: Installing a new G700 without an S8300 using the Gateway Installation Wizard](#)
- [Chapter 5: Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool](#)
- [Chapter 6: Upgrading an existing G700 without an S8300 using the Upgrade Tool](#)

Following these chapters is a chapter covering the installation of telephones and adjunct systems that are performed as part of any installation. This chapter is:

- [Chapter 7: Telephones and adjunct systems](#)

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

- [Chapter 8: Manual installation of a new G700 with an S8300](#)
- [Chapter 9: Manual installation of a new G700 without an S8300](#)
- [Chapter 10: Manual upgrade of an S8300A and G700 to R4.0](#)
- [Chapter 11: Manual upgrade of an existing S8300B or S8300C and G700 to R4.0](#)
- [Chapter 12: Manual upgrade of an existing S8300B and G700 to S8300C with R4.0](#)
- [Chapter 13: Manual upgrade of an existing G700 without an S8300 to R4.0](#)

Read [Chapter 1: Roadmaps and reference information](#), before you begin the installation.

Chapter 1 contains checklists for the four installation and upgrade scenarios. Then read and follow the procedures in the chapters that apply to the installation or upgrade scenario you are working with. Chapter 1 also contains information on alternative methods to connect to and access a G700 system.

Read [Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server](#) for instructions on installing and cabling the hardware.

Read [Chapter 7: Telephones and adjunct systems](#) if you need to install phones or adjuncts.

Chapter 8 covers the IA 770 INTUITY AUDIX Messaging Application, the INTUITY LX Messaging System, the G700 Sourced Announcements, Avaya Integrated Management, the Uninterruptible Power Supply (UPS), Universal Serial Bus (USB) Modems, and other adjuncts.

See the following appendices for system specifications, forms you must complete for the installation, and comcodes and other information that you need to order equipment:

- [Appendix A: Technical information](#) contains specifications and other technical information that you need to install an S8300 Media Server with a G700 Media Gateway.
- [Appendix B: Information checklists](#) contains the pre-installation worksheets that you will need to have filled in before you start an installation or upgrade.
- [Appendix C: Equipment list](#) contains the information that you need to order equipment.
- [Appendix D: Install the Avaya TFTP server](#) contains instructions for installing and configuring the Avaya TFTP Server software.

Conventions

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

Physical dimensions

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

Terminology

- *System* — a general term encompassing all references to the Avaya servers running Avaya Communication Manager.

- Circuit pack codes (for example, TN780 or TN2182B) are shown with the *minimum acceptable* alphabetic suffix (like the “B” in the code TN2182B).

Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every *vintage* of either the minimum suffix or a higher suffix code is necessarily acceptable. A suffix of “P” means that firmware can be downloaded to that circuit pack.

- *ASAI* — a term synonymous with the newer CallVisor ASAI.
- *UUCSS* — a code that refers to a circuit pack address in cabinet-carrier-slot order.
nnnVxx is the code that refers to a media module address in gateway-V-slot order.

Recent terminology changes that are important to note include:

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

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

- *Service pack* — a software update.

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

Typography

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

Commands

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

Example:

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

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

Example:

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

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

Example:

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

Keys

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

Example:

Use the **Down Arrow** key to scroll through the fields.

- When you must press and hold a key and then press a second or third key, we separate the names of the keys are separated with a plus sign (+).

Example:

Press **ALT+D**.

- When you must press two or more keys in sequence, we separate the names of the keys are separated with a space.

Example:

Press **Escape J**.

- When you must press a function key, we provide the function of the key in parentheses after the name of the key.

Example:

Press **F3 (Save)**.

User input

- User input is in **bold** type, whether you must type the input, select the input from a menu, or click a button or similar element on a screen or a Web page.

Example:

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

System output and field names

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

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

Example:

- The system displays the following message:
The installation is in progress (Web output)
`The installation is in progress` (CLI output)
- Type **y** in the **Message Transfer?** field.

Downloading this book

You can view or download the latest version of the *Installing and Upgrading the Avaya G700 Media Gateway and Avaya S8300 Media Server*, 555-234-100, from the Avaya Web site at: <http://support.avaya.com>. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Support Web site.

Safety labels and security alert labels

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

**CAUTION:**

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

**WARNING:**

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

**WARNING:**

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

**DANGER:**

A danger statement calls attention to a situation that can result in harm to personnel.

**SECURITY ALERT:**

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

Related resources

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

For a summary of what is new in the February 2007 release of Avaya Communication Manager, see *What's New in Avaya Communication Manager for Release 4.0*, 03-300682.

About this book

For more information on the Avaya G700 Media Gateway and related features, see the following books:

Title	Number
Hardware Description and Reference for Avaya Communication Manager	555-245-207
Overview for Avaya Communication Manager	03-300468
Maintenance Commands for Avaya Communication Manager 4.0, Media Gateways and Servers	03-300431
Maintenance Alarms for Avaya Communication Manager 4.0, Media Gateways and Servers	03-300430
Maintenance Procedures for Avaya Communication Manager 4.0, Media Gateways and Servers	03-300432
Quick Start for Hardware Installation: Avaya S8300 Media Server and Avaya G700 Media Gateway	555-233-150

Technical assistance

Avaya provides the following resources for technical assistance.

Within the United States

For help with:

- Feature administration and system applications, call the Avaya Technical Consulting - System Support at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353
- Security issues, call Avaya Corporate Security at 1-877-993-8442

International

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

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

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Ordering Documentation

In addition to this book, other description, installation, maintenance, and administration books, and documentation library CDs, are available.

This document (555-234-100) and any other Avaya documentation can be ordered directly from the Avaya Publications Center toll free at 1-800-457-1235 (voice) and 1-800-457-1764 (fax). International customers should use +1.207.866.6701 (voice) and +1.207.626.7269 (fax).

Sending us comments

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

- Mail, send your comments to:

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

- E-mail, send your comments to:

document@avaya.com

- Fax, send your comments to:

1-303-538-1741

Ensure that you mention the name and number of this book, *Installing and Upgrading the Avaya G700 Media Gateway and Avaya S8300 Media Server*, 555-234-100.

Section 1: Reference information and hardware installation

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

- [Chapter 1: Roadmaps and reference information](#)
- [Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server](#)

Chapter 1: Roadmaps and reference information

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

This Chapter is organized as follows:

- [What wizards are available](#)
- [About connection and login methods](#)
- [About navigation for G700 CLI commands](#)
- [About terminal emulation function keys for Communication Manager](#)

What wizards are available

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

- Avaya Installation Wizard
See *Job Aid: Avaya Installation Wizard*, 555-245-754.
- Gateway Installation Wizard
See *Job Aid: Avaya Gateway Installation Wizard*, 555-245-756.
- Upgrade Tool
See *Job Aid: Upgrade Tool and Worksheets*, 555-245-757.
- Software Update Manager
See *Avaya Software Update Manager User Guide*, 14-300168.

Note:

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

Where are the most recent versions of the Wizards

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



Tip:

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

When to use each wizard

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

About connection and login methods

This section describes the various ways of connecting to, and logging into, the Avaya™ S8300 Media Server and the Avaya™ G700 Media Gateway. Use this chapter as a reference for the other chapters in this book.

The procedures in this book assume that you are connecting to the S8300 and/or the G700 with an Avaya Services laptop. However, the methods apply for any type of PC.

This chapter is organized as follows:

- [What physical access methods are available](#)
- [Laptop configuration for direct connection to the services port](#)
- [About connection methods](#)
- [About Log in Methods](#)
- [About navigation for G700 CLI commands](#)

What physical access methods are available

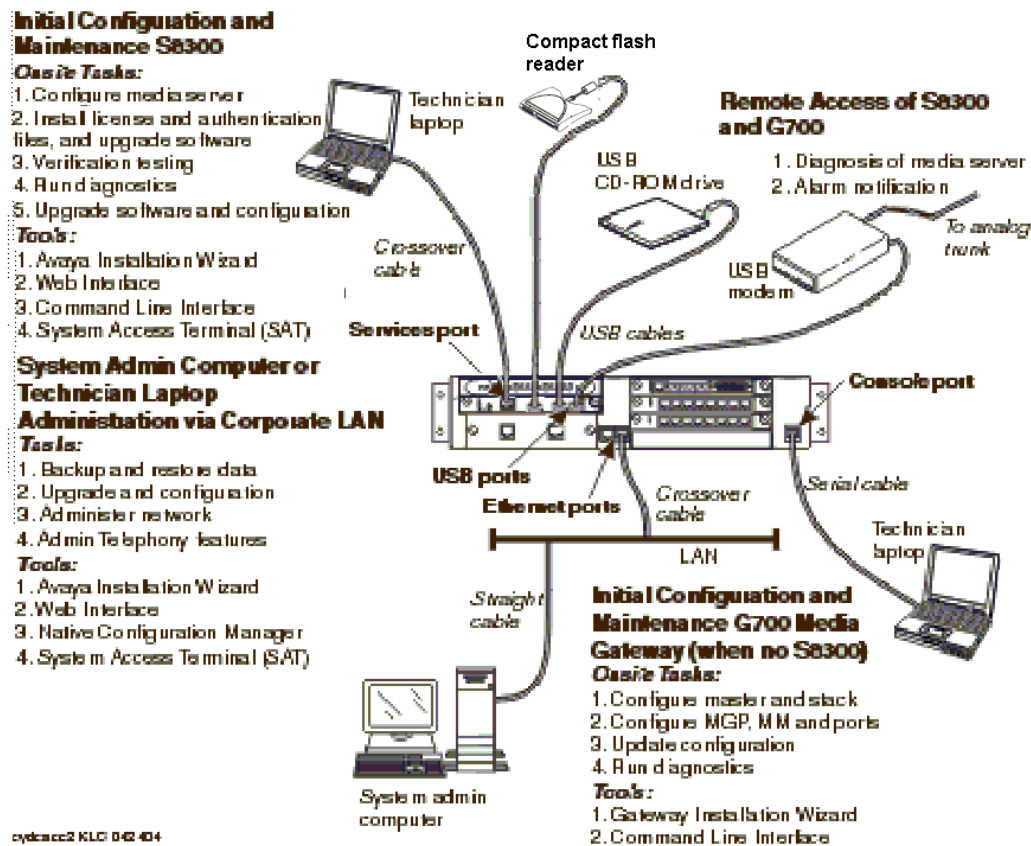
[Figure 1](#) reviews physical access methods for the S8300 and G700. Check for the locations of the following ports:

- If the S8300 is present in the G700,
 - Services port in the center of the S8300
 - USB ports on the right side of the S8300
- If the S8300 is not present in the G700,
 - Ethernet ports (EXT 1/ EXT 2) in the bottom center of the G700

You will need to connect the G700 to the customer's LAN using one of these ports for loading the latest software.

- Console port at the lower right of the G700

Figure 1: Summary of S8300 and G700 Access Methods and Tasks



Laptop configuration for direct connection to the services port

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

Note:

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

What network settings are required on the laptop

A laptop connected directly to the Services Ethernet interface on the S8300, S8400, S8500, or S8700/S8710/S8720 Media Server requires a specific configuration as described in this section.

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

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

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

Configuring the laptop for a direct connection

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

Note:

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

To check your version of windows

1. Log in to your laptop, and double-click the **My Computer** icon on your desktop.
The My Computer window opens.
2. Click **Help** on the My Computer window's toolbar.
The Help menu opens and displays the version of Windows installed on your laptop.
3. Follow one of the two procedures below, depending on your operating system.

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

1. Right-click My Network Places on your desktop or under the Start menu in XP.
2. Select **Properties** to display the **Network and Dial-up Connections** window.
Windows should have automatically detected the Ethernet card in your system and created a LAN connection for you. More than one connection may appear.
3. Right-click the correct **Local Area Connection** from the list in the window.

4. Select **Properties** to display the **Local Area Connection Properties** dialog box.
5. Select **Internet Protocol (TCP/IP)**
6. Click the **Properties** button.

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

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

Note:

Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.

8. Disable DNS service as follows:
 - a. Click the radio button labeled **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
 - b. Click the **Advanced** button at the bottom of the screen.

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

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

The **address** field should be blank.

9. Disable WINS Resolution as follows:

- a. Click the **WINS** tab. Make sure WINS is not administered.

The **address** field should be blank.

- b. Click **OK**.

If warned about an empty primary WINS address, click **Yes** to continue.

10. Click **OK** twice to accept the address information and close the **TCP/IP** and **Local Area Connection Properties** dialog boxes.

11. Reboot the system if directed to do so.

After you have made these changes to your computer's network configuration information, the **Network and Dial-up Connections** window shows the status of the **Local Area Connection**:

- **Enabled** appears when the laptop's Ethernet cable is connected to the server.
- **Disabled** or **unplugged** appears if the NIC is not connected to anything.

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

1. Access your computer's network information.

On your desktop:

- *Windows 95, 98, and NT*: Right-click **Network Neighborhood**.
- *Windows ME*: Right-click **My Network Places**.

2. Select **Properties** to display the Network dialog box.

3. Locate the TCP/IP properties as follows:

- *Windows 95, 98, and ME*: On the **Configuration** tab, scroll through the installed network components list to the TCP/IP part of the devices list. Select the TCP/IP device that corresponds to your Ethernet card.
- *Windows NT*: On the Protocols tab, select **TCP/IP** in the installed network components list.

4. Select the **Properties** button.

5. In the TCP/IP Properties box, click the **IP Address** tab.

6. Click the radio button to **Specify an IP address**.

Enter the following:

- IP address: **192.11.13.5**
- Subnet mask: **255.255.255.252**

Note:

Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.

7. Disable DNS service as follows:

- *Windows 95, 98, and Me*: Click the **DNS Configuration** tab. Verify that the **Disable DNS** radio button is selected.
- *Windows NT*: Click the **DNS** tab.
 - a. If any IP addresses appear under **DNS Service Search Order**, make a note of them in case you need to restore them later.
 - b. Select each IP address in turn and click the **Remove** button.

8. Disable WINS Resolution as follows:

- *Windows 95, 98, and Me*: Click the **WINS Configuration** tab. Verify that the **Disable WINS Resolution** radio button is selected.
- *Windows NT*: Click the **WINS Address** tab.
 - a. If any IP addresses appear for the Primary and Secondary WINS servers, make a note of them in case you need to restore them later.

- b. Clear each server entry.
 - c. Clear the checkbox for **Enable DNS for WINS Resolution**.
9. Click OK twice to accept the address information and close the **Network** dialog box.
10. Reboot the system if directed to do so.

Disabling or bypassing proxy servers in Web browser

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

Note:

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

To check or change proxy settings

1. Open your Internet browser.
2. Verify that you have a direct connection with no proxies, using one of the following options:
 - **For Internet Explorer:**
 - a. Select **Tools > Internet Options**.
 - b. Click the **Connections** tab.
 - c. Click the **LAN Settings** button.
 - d. If **Use a proxy server for your LAN** is not selected, no change is necessary; click **Cancel** to exit.
 - e. If **Use a proxy server for your LAN** is selected, you can:
 - Deselect it and click **OK** to exit
 - or,
 - Leave it selected and configure your browser to bypass the proxy server whenever you are connected to the S8300 services port:
 - i. Click **Advanced**
 - ii. Type **192.11.13.6** in the Exceptions box. If there are other entries in this box, add to the list of entries and separate entries with a “,”.
 - iii. Click **OK** to exit.

- **For Netscape:**
 - a. Select **Edit > Preferences**.
 - b. Under Category, click **Advanced**.
 - c. Click **Proxies**.
 - d. If **Direct connection to the Internet** is selected, no change is necessary; click **Cancel** to exit.
 - e. If **Direct connection to the Internet** is not selected, you can:
 - select it and click **OK** to exit
 - or,
 - Leave it unselected and configure your browser to bypass the proxy server whenever you are connected to the S8300 services port:
 - i. Select **Manual Proxy Configuration** and click **View**
 - ii. Type **192.11.13.6** in the **Exceptions** box (or in the **No Proxy for:** box in later versions of Netscape). If there are other entries in this box, add to the list of entries and separate entries with a ";".
 - iii. Click **OK** to exit.

About connection methods

Connecting a laptop to services port of S8300

To connect your laptop directly to the S8300 media server

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

Table 1: Crossover cable pinout chart

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

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

Connecting a laptop to the G700 serial port

To configure a G700 that *does not have an S8300*, you may need to set up a direct connection from your laptop's serial port to the G700 Console (serial) port.

To connect a laptop directly to the serial port on the G700 media gateway

1. For a stacked configuration, locate the device that contains the master controller for the stack.

Check the LED panel on the upper left of each G700 or C360 device in the stack as follows:

- G700 Media Gateway: a lit **MSTR** LED indicates that this unit is the stack master.
 - A non-G700, C360 device: a lit **SYS** LED indicates that this unit is the stack master.
2. Connect the RS-232 serial cable and DB-9 adapter cable provided with the G700 between your laptop and the G700.
 - a. Attach one end of the RS-232 cable to the RJ-45 jack on the front of the G700 that is the stack master. The serial port is on the lower right side of the chassis, labeled **Console**.
 - b. Plug the other end of the RS-232 cable into the RJ-45 jack on the DB-9 adapter cable.
 - c. Connect the other end of the DB-9 adapter cable to the 9-pin serial port on your laptop.
 3. Use a serial-connection program such as HyperTerminal to access the P330 Stack Processor.

Connecting a laptop to the customer LAN

To connect to the customer's LAN, either on site or remotely over the Internet, your PC must be assigned an IP address on the LAN. The IP address can be a static address on the customer's LAN that you enter in the TCP/IP properties or it can be assigned dynamically with DHCP. Ask the customer how they want you to make the connection.

Connecting an external modem to the S8300 media server

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

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

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

To set up a dial-up connection

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

Note:

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

4. Verify operation as instructed by the modem's documentation.
5. To enable the modem, access the S8300 Media Server's Maintenance Web Pages (see [Logging in to the S8300 Web Interface from your laptop](#) on page 57), and click Enable/Disable Modem on the main menu

The system displays the Enable/Disable Modem window.

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

The modem is now ready to receive calls.

Setting up Windows for modem connection to the media server (Windows 2000 or XP)

Note:

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

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

1. Right-click **My Network Places** and click **Properties**.
2. Click **Make New Connection** and follow the Network Connection Wizard:
3. Select **Dial-up to private network** on the **Network Connection Type** screen.
4. In the **Phone number** field, enter the appropriate telephone number inserting special digits such as 9 and 1 or *70, if necessary.
5. On the **Connection Availability** screen, click **For all users** or **Only for myself**, as appropriate.

6. On the **Completing the Network Connection Wizard** screen, type the name you want to use for this connection. This name will appear in the **Network and Dial-up Connections** list.
7. Check the **Add a shortcut to my desktop**, if desired, and click **Finish**.
8. If a **Connect** screen appears, click **Cancel**.

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

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

1. On your PC's desktop, right-click **My Network Places** and click **Properties**.
The system deploys the **Network and Dial-up Connections** window.
2. Double click the connection name you made in the previous task, [Setting up Windows for modem connection to the media server \(Windows 2000 or XP\)](#).

Note:

Depending on your system, the **Connect** screen may appear, from which you must select **Properties**.

3. Click the **Security** tab.
4. Select the **Advanced (custom settings)** radio button.
5. Check the **Show terminal window** checkbox.
6. Click the **Networking** tab.
7. In the **Components** box, verify that **Internet Protocol (TCP/IP)** and **Client for Microsoft Networks** are both checked.
8. Select **Internet Protocol (TCP/IP)** and click **Properties**.
9. Click the **Advanced** button.
10. Uncheck (clear) the **Use default gateway on remote network** box.
11. Click **OK** three times to exit and save the changes.

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

Note:

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

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

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

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

Using Avaya Terminal Emulator for LAN Connection to Communication Manager

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

To use Avaya Terminal Emulator for LAN connection to Communication Manager

1. Double-click the **Terminal Emulator** icon on your desktop. Alternatively, go to the Start menu, select **Programs**, then select **Avaya**, and finally select **Terminal Emulator**. The system displays the Terminal Emulator.
2. From the menu bar at the top of the screen, select **Phones**, then select **Connection List**.
The system displays the **Connections** window.
3. From the menu bar across the top, select **Connection**, then select **New Connection**.
The system displays the **Connection Settings** window.
4. Put in a name for the connection. Usually, this will be the name of your media server.
5. In the **Host** window, click **Telnet**.

Note:

Telnet is turned off by default in Communication Manager. To log in with Telnet, you must turn Telnet on with the Firewall Web page in Communication Manager.

6. Click the **Emulation** tab at the top.
The system displays the **Emulation** tab.
7. From the Emulator dragdown box, select the emulator you desire, usually 513BCT (default), AT&T 4410, AT&T or DECVT100.
8. In the **Keyboard** window, select **pbx**.
9. Click the **Network** tab.
The system displays the **Network** tab.
10. In the IP address field, type the IP address of the media server.
11. In the TCP/IP port number field, leave **23** if you want to log in at the Linux command line.
Type **5023** if you want to log in directly to the Communication Manager SAT command line.
12. Click **OK**.
The **Connection Settings** window disappears.
13. On the **Connections** window, double-click the name of the connection you just set up.
 - If you used port **5023**, the Login prompt for the Communication Manager software appears.
 - If you used port **23**, the Login prompt for the S8300 Linux software appears.

14. Log in to Communication Manager to access the SAT command prompt screen. If you are logging in as *craft*, you log in to the S8300 Linux software. Then, see [Open the Communication Manager SAT Screens](#) on page 62.

Using Avaya Terminal Emulator for Modem Connection to Communication Manager

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

To use Avaya Terminal Emulator for Modem Connection to Communication Manager

1. Complete steps 1–8 in [To use Avaya Terminal Emulator for LAN connection to Communication Manager](#) on page 53.
2. Click the **Modem** tab.
The system displays the **Modem** tab.
3. In the IP address field, type the IP address of the connection's **Dialup Status** box as noted in Step 9 in [To use Windows for PPP modem connection \(Windows 2000 or XP\)](#).
4. In the **TCP/IP Port Number** field, leave **23** if you want to log in at the Linux command line. Type **5023** if you want to log in directly to the Communication Manager SAT command line.
5. In the **Modem** field, use the dragdown box to select the type of modem that your PC uses.
6. In the **Serial port** field, select the **COM** port you are using for your modem connection.
7. In the **Baud rate** field, select **9600** from the dragdown box.
8. Click the **Dial Numbers** tab.
The system displays the **Display Numbers** tab.
9. Type the phone number of the media server as appropriate. Enter 1 in the **Country Code** field for long-distance.
10. Click **OK**.
11. On the **Connections** window, double-click the name of the connection you just set up.
The PC dials up the media server, and when connected, the login prompt for the Communication Manager software appears.
12. Log in to Communication Manager to access the SAT command prompt screen. If you are logging in as *craft*, you log in to the S8300 Linux software. Then, see [Open the Communication Manager SAT Screens](#) on page 62.

About Log in Methods

This section describes how to log on to the S8300, S8400, S8500, or S8700/S8710/S8720 media servers using SSH (Secure Shell), Telnet, or the built-in Web Interface and how to start a SAT session. The last procedure in this section describes logging in to the P330 Stack Processor when you have a direct serial connection to the G700 Console port.

These procedures assume:

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

or,

- You are connected to the S8300, S8400, S8500, or S8700/S8710/S8720 media server over the customer's LAN, either remotely or on site.

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

Accessing the server's command line interface with SSH

To use this procedure with a laptop cable connection to the services port, you must configure your laptop for the network connection. See [Configuring the laptop for a direct connection](#) on page 43. In addition, a third-party SSH client must already be installed on your computer. PuTTY is one such client available for download from <http://www.putty.nl/download.html>.

Note:

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



CAUTION:

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

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

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

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

2. In the **Host Name (or IP address)** field, type **192.11.13.6** if connecting to the services port. Otherwise, for access over the LAN/WAN, type the IP address or the host name of the server.
3. In the **Port** field, type **22**.

4. Under **Protocol**, select **SSH**.
5. In the PuTTY menu on the left, click **Connection>SSH**.
The Options controlling SSH connections dialog box opens.
6. In the **Preferred SSH protocol version** field, select **2**.
7. In the **Encryption options** window, use the up and down arrows to set **AES (SSH-2)** as the top option and **3DES** as the second option.

Note:

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

8. Click **Open**.

Note:

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

When connecting through the services laptop interface, if you save the host key, the host will be identified as 192.11.13.6. If you later connect to a different server through its laptop interface, this new host also appears as 192.11.13.6, but it will have a different key. You get a prompt in this case because it appears that the host key has changed.

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

The system displays the **PuTTY** window.

10. Log in as **craft**.

Logging in to the media server from your laptop using Telnet

Note:

Telnet is turned off by default in Communication Manager. To log in with Telnet, you must turn Telnet on with the Firewall Web page in Communication Manager.

To run telnet

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

For example:

- a. On a Windows system, go to the **Start** menu and select **Run**.
- b. Type **telnet 192.11.13.6** to access the media server CLI.

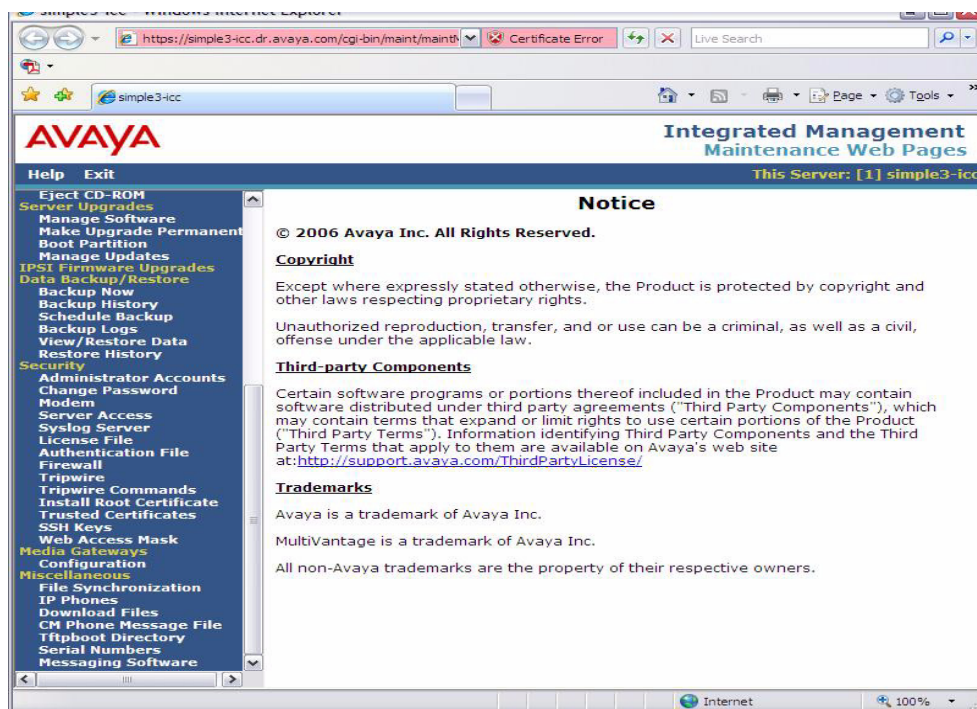
3. When the **login** prompt appears, type the appropriate user name (for example, *cust* or *craft*).
4. When prompted, enter the appropriate password.
5. If you log in as *craft*, you are prompted to suppress alarm origination.
Generally you should accept the default value (yes).
6. Enter your terminal type.
Accept the default value, or enter the appropriate type for your computer. For example, you may use type **ntt**, a terminal type available for Windows NT4.0 or Windows 98. For Windows 2000, use **w2ktt**.
7. If prompted for a high-priority session, typically answer **n**.
The system displays the telnet prompt. It may take the form `<username@devicename>`.

Logging in to the S8300 Web Interface from your laptop

To run the Web Interface

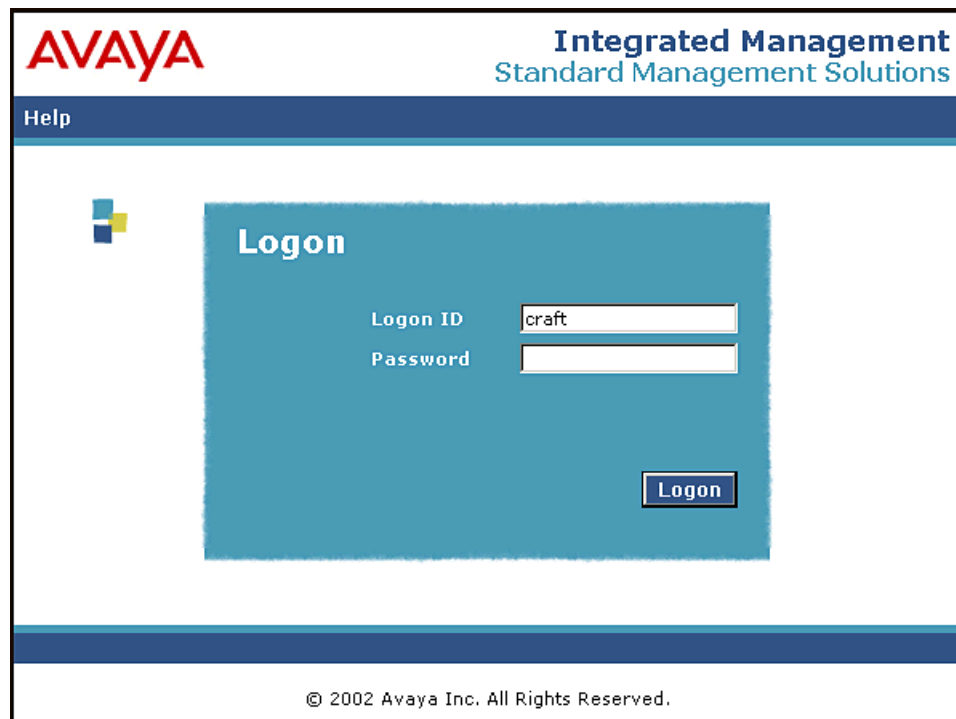
1. Open Internet Explorer (5.5 or later) on your computer.
2. In the Address (or Location) field of your browser, type the **192.11.13.6** (or, for a LAN connection, the IP address of the media server on the customer LAN) and press **Enter**.
If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate.
3. The system displays the **Welcome** screen.

Welcome Screen



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

Login Screen



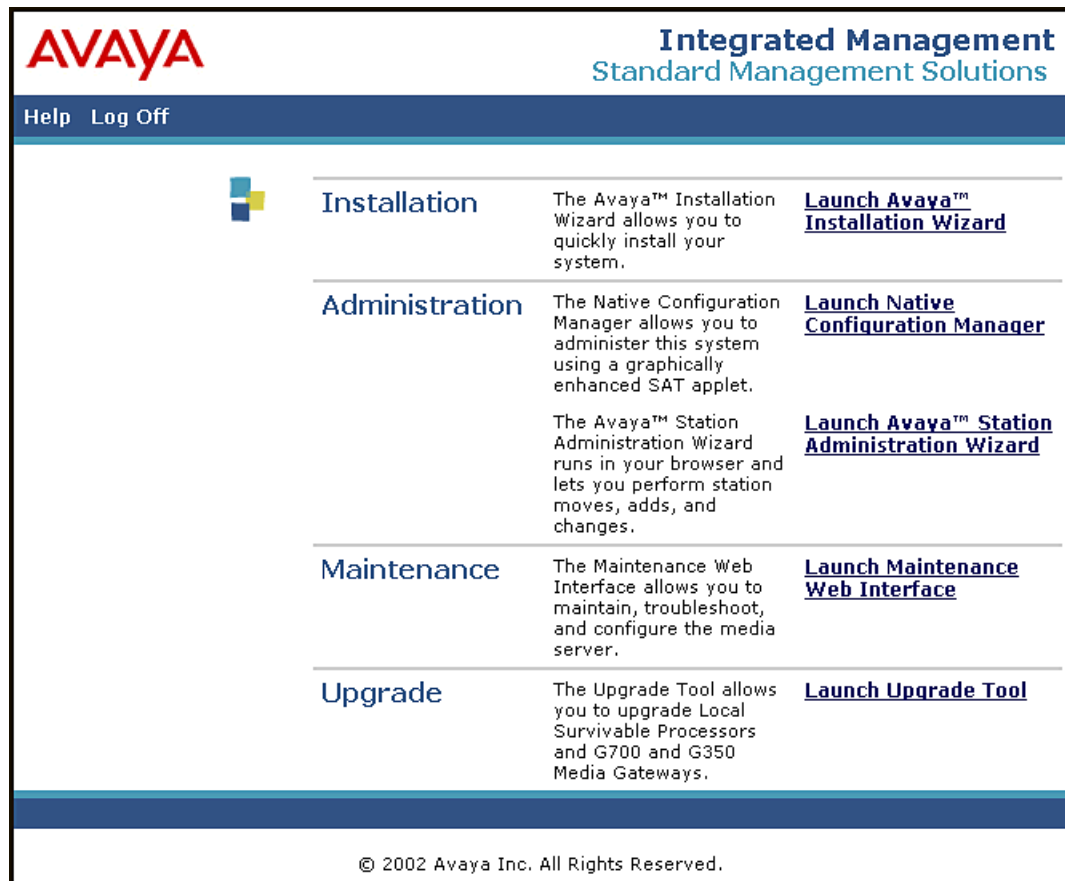
The screenshot shows the login interface for the Avaya Integrated Management Standard Management Solutions. At the top left is the AVAYA logo in red. To its right, the text "Integrated Management" is in bold blue, and "Standard Management Solutions" is in a lighter blue. Below this is a dark blue horizontal bar with the word "Help" in white. The main content area has a light blue background. On the left side of this area is a small icon consisting of three squares (two blue, one yellow). To the right of the icon is a white rectangular box with a blue border. Inside this box, the word "Logon" is written in bold blue at the top. Below it, there are two labels: "Logon ID" and "Password". Next to "Logon ID" is a text input field containing the word "craft". Next to "Password" is an empty text input field. At the bottom right of the white box is a blue button with the word "Logon" in white. Below the main content area is another dark blue horizontal bar. At the very bottom of the page, centered, is the copyright notice: "© 2002 Avaya Inc. All Rights Reserved."

6. Log in as *craft*.

7. Select **yes** for Suppress Alarm Origination.

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

Main Menu



The screenshot shows the Avaya Integrated Management Standard Management Solutions main menu. The header features the Avaya logo on the left and the product name on the right. Below the header is a navigation bar with 'Help' and 'Log Off' links. The main content area is divided into four sections: Installation, Administration, Maintenance, and Upgrade. Each section contains a brief description and a link to launch the respective tool. The footer displays the copyright notice: © 2002 Avaya Inc. All Rights Reserved.

Section	Description	Launch Link
Installation	The Avaya™ Installation Wizard allows you to quickly install your system.	Launch Avaya™ Installation Wizard
Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet. The Avaya™ Station Administration Wizard runs in your browser and lets you perform station moves, adds, and changes.	Launch Native Configuration Manager Launch Avaya™ Station Administration Wizard
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade Local Survivable Processors and G700 and G350 Media Gateways.	Launch Upgrade Tool

8. Click on the link for **Launch Maintenance Web Interface**

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

S8300 Main Menu/Usage Agreement Notice

AVAYA Integrated Management Maintenance Web Pages

Help Exit This Server: [1] simple3-icc

Notice

© 2006 Avaya Inc. All Rights Reserved.

Copyright

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

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

Third-party Components

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

Trademarks

Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

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

https://simple3-icc.dr.avaya.com/cgi-bin/maint/maintLegalNotice#

9. Check the top of the left panel. Note that:

- The Avaya media server you are logged into is identified by name and server number.
- The S8300 media server number is always 1.

Open the Communication Manager SAT Screens

To run SAT:

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

Or, to open SAT directly from your laptop:

- a. Run PuTTY or another SSH client.
- b. Use IP address **192.11.13.6** and port number **5023**.

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

Enter your login confirmation information as prompted:

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

3. Enter your terminal type.

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

The system displays the SAT interface.

4. Enter SAT commands as appropriate.

Logging in to the P330 Stack Processor with a Direct Connection to the S8300 Services Port

Note:

If you are upgrading an S8300/G700 remotely, connect to the customer LAN and telnet to the IP address of the P330 stack master (that is, the P330 Stack Processor running as the stack master). The IP address is the address assigned on the customer LAN, not 192.11.13.6.

To log in with a direct connection to the S8300 services port:

1. With a direct connection to the S8300 services port, SSH to the S8300 IP address with PuTTY or another SSH client, using the IP address **192.11.13.6**.
2. Login as *craft* or *cust*.
3. Telnet to the P330 stack master stack processor.

Type **telnet <xxx.xxx.xxx.xxx>**, where **<xxx.xxx.xxx.xxx>** is the IP address of the P330 stack master processor on the customer's LAN.

4. Login at the **Welcome to Avaya P330** screen.

Login: *xxx from the planning documentation*

Password: *xxx from the planning documentation*

You are now logged-in at the Supervisor level. The prompt appears as **P330-1(super)#**.

Note:

To check the syntax of a command in the command line interface, type as much of the command as you know followed by **help**. For example:

P330-1(super)#> set help

you will be given the current list of **set** commands available. If you type:

P330-1(super)#> set interface help

you will be given a much more restricted list of command possibilities that address the possible interfaces to be set.

For a complete list of command line interface commands, type **help** or refer to the *Avaya P330T User's Guide* (available at <http://www.avaya.com/support>).

Logging in to the P330 Stack Processor with a LAN Connection

To log in with a LAN connection:

1. With a connection to the customer's LAN (either remotely or on site), telnet to the P330 Stack Processor IP address.

Type **telnet <xxx.xxx.xxx.xxx>**, where **<xxx.xxx.xxx.xxx>** is the IP address of the P330 stack master processor on the customer's LAN.

2. Login at the **Welcome to Avaya P330** screen.

Login: *xxx from the planning documentation*

Password: *xxx from the planning documentation*

You are now logged-in at the Supervisor level. The prompt appears as **P330-1(super)#**.

Logging in to the P330 Stack Processor with a Direct Serial Connection

Use this procedure to access the G700 processors when your laptop is directly connected to the Console port using a serial cable.

To access the G700 using the Console (serial) port

1. Launch Windows® HyperTerminal or any other terminal emulation program.

Note:

For most Windows-based PCs, you access the HyperTerminal program from the **Start** menu by selecting **Programs**, then **Accessories**.

2. Choose **Call - Connect** (for HyperTerminal) or the appropriate call command for your terminal emulation program.
3. Login at the **Welcome to Avaya P330** screen.

Login: *xxx from the planning documentation*

Password: *xxx from the planning documentation*

You are now logged-in at the Supervisor level. The prompt appears as **P330-1(super)#**.

Logging in to the P330 Stack Processor with Device Manager

To access the Device Manager, you must have access to the corporate LAN in which the P330 Stack Processor resides.

To access Device Manager, do the following:

1. Open a compatible Internet browser on your computer.

Currently this includes Internet Explorer 5.0 (or higher) and Netscape Navigator 4.7 and 6.2. The Java Plug-in 1.2.2 or 1.3.1 is required.

2. In the **Address** (or **Location**) field of your browser, type the IP address or name of the P330 Stack Processor and press **Enter**.

If the network includes a domain name service (DNS) server that has been administered with this IP device's name, you can type the processor's name into the address field instead of the IP address. For example, **http://P330-stack1.mycompany.com**

Note:

The Device Manager is *not* available through the S8300 Media Server. You must be connected to either the P330 Stack Processor or G700 Media Gateway processor through the corporate LAN.

A GUI rendering of the stack devices appears.

3. Proceed with Media Gateway or stack device administration.

About Avaya Site Administration

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

Configuring Avaya Site Administration

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

When it runs initially, after downloading, you need to create a new entry for the switch connection. To create new entries for the switch, follow the procedure [To add an S8300 switch administration item](#) on page 65.

To add an S8300 switch administration item

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

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

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

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

3. Click **Next**.

The **Connection Type** dialog box displays.

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

5. Click **Next**.

The **Network Connection** dialog box displays.

6. Enter the IP address used to connect to the S8300.

7. Click **Next**.

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

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

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

9. Click **Next**.

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

10. Click **Next**.

The **Login Type** dialog box displays.

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

12. Click **Next**.

The **Switch Summary** dialog box displays.

13. Check the information.

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

14. Click the **Test** button to test the connection.

15. When the connection is successfully tested, click **Next**; and then, **Finish**.

Logging in to the S8300 with ASA

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

To start Avaya Site Administration

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

About navigation for G700 CLI commands

[Table 2](#) describes a few Command Line Interface commands that you will need to navigate among the processors on the G700.

Note:

This navigational aid assumes that you are logged in to the P330 Stack Processor. Default mode is **Supervisor** with a **P330-1(super)#** command-line prompt.

Table 2: Navigational aid for G700 CLI commands

Command	Purpose	Prompt
super	change to supervisor mode	P330-y(super)# or <MG-xxx>-y(super)# where xxx is the media gateway number assigned on the add media-gateway form, and y is the "module number" of the G700 in the stack.
configure	change to configuration mode	P330-1(configure)# or <MG-001>-1(configure)#
session <module #> mgp (from a stack processor session)	open a CLI session on the mgp processor	<MG-001>-1(super)#
session <module #> stack (from an MGP session)	open a CLI session on the stack processor	P330-1(super)#
session icc (from an MGP session)	open a CLI session on the S8300 processor	craft@<host name>>
session <#>	open a session on the stack processor in module (i.e. another G700)<#> in the stack	P330-<#>(super)#
exit	close the current session (and revert to the previous session)	
<command> help	displays help for <command>	

The command-line prompts in an MGP session use the media gateway name that is assigned when the gateway is configured.

You can telnet to another processor from a current telnet session.

About terminal emulation function keys for Communication Manager

When you log in to the Communication Manager SAT screens, your terminal emulation may not display function keys on the screen to help you determine which function keys to press. Use [Table 3](#) as a guide for **ntt** terminal emulation.

Table 3: Key sequences for ntt terminal emulation

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

[Table 4](#) lists key presses for **w2ktt** terminal emulation.

Table 4: Key sequences for w2ktt terminal emulation

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

Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server

Configurations using the G700 media gateway consist of three main elements:

- G700 Media Gateway
- S8300, S8400, S8500, or S8700/S8710/S8720 Media Server
- Avaya Communication Manager software

The chapter is organized in two main sections:

- [About hardware components](#) - Describes the G700 and S8300 components.
- [About installation and cabling](#) - Provides hardware installation and cabling procedures.

Note:

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

About hardware components

This section describes the components of an Avaya G700 Media Gateway and an Avaya S8300 Media Server.

What are the main elements of the G700 media gateway

The main elements of a G700 Media Gateway are:

- G700 chassis and processors
- Media modules
- Avaya Data Expansion Modules

Figure 2: G700 media gateway with an S8300 media server: front view

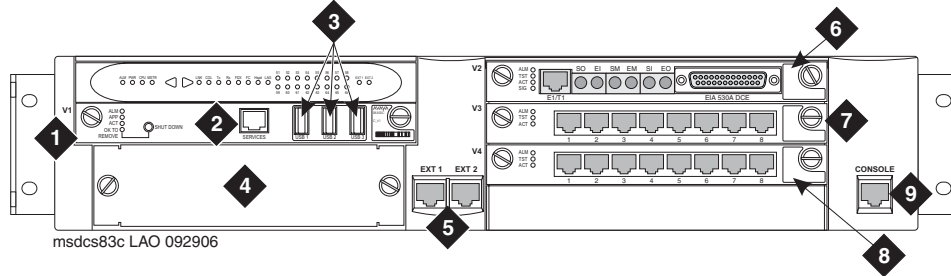


Figure notes:

1. Media module slot #1 (V1)	5. 10/100 Base-T Ethernet ports (ext1, ext2)
2. S8300 services port (used with cross-over ethernet cable)	6. Media module slot #2 (V2)
3. S8300 USB ports (S8300C shown)	7. Media module slot #3 (V3)
4. Expansion module slot	8. Media module slot #4 (V4)
	9. Console interface

What comprises the G700 media gateway chassis and processors

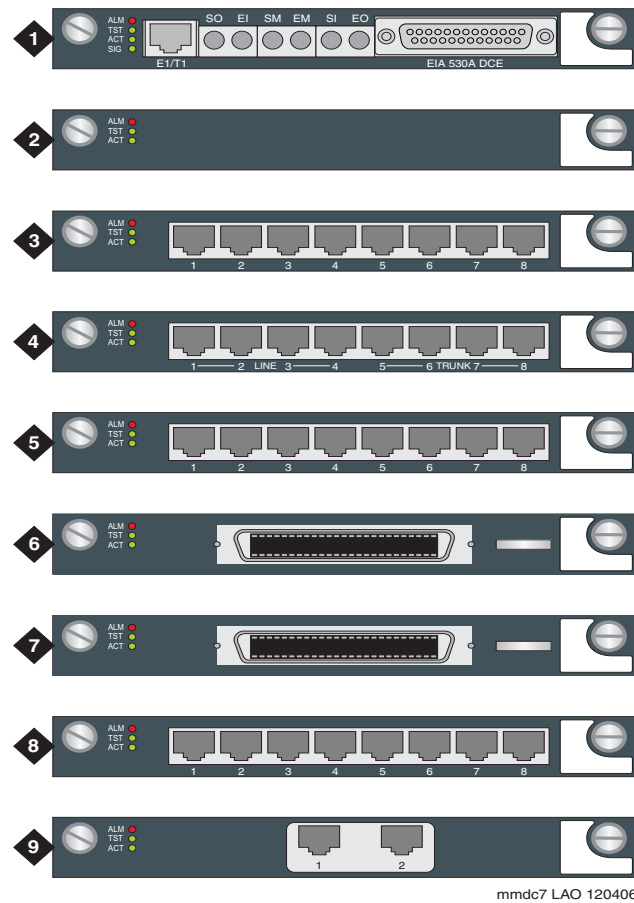
The G700 Media Gateway chassis is a 19-inch, 2u rack-mountable unit. A partial list of technical specifications of the G700 appears in [Appendix A: Technical information](#).

The G700 has three internal processors:

- P330 Stack Processor (also known as *Layer 2 switching processor*)
- Media gateway processor (MGP)
- Voice over IP (VoIP) processor

What are the media modules

Media modules are optional, plug-in circuit assemblies. They provide traditional interfacing of service provider network access solutions (such as T1/E1) and connections to TDM-based endpoints (such as DCP digital phones and analog phones). The available media modules are (as shown in [Figure 3: Media modules](#) on page 71):

Figure 3: Media modules**Figure notes:**

1. Avaya MM710 T1/E1 Media Module
2. Avaya MM760 VoIP Media Module for additional VoIP resources
3. Avaya MM711 Analog Media Module for connection to 8 analog stations or CO trunks
4. Avaya MM714 Analog Media Module for connection to 4 analog stations and 4 CO trunks. Analog DID trunk connections are to be associated with the ports labeled "Line" and not "Trunk".
5. Avaya MM712 DCP Media Module for connection to 8 DCP stations
6. Avaya MM716 Analog Media Module for connection to 24 analog stations
7. Avaya MM717 DCP Media Module for connection to 24 DCP stations (*see the Caution below* for limitations on the use of the MM717)
8. Avaya MM720 BRI Media Module for connection to 8 ports for international BRI trunks or BRI endpoint (telephone and data module) connections
9. Avaya MM722 BRI Media Module for connection to 2 ports for international BRI trunks

For detailed descriptions of the media modules see *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207.

! CAUTION:

A maximum of 3 MM717 24-port DCP Media Modules can be installed in a single G700. Also, the ports on the MM717 are intended for in-building use only. Phone lines connected to those ports are not to be routed out-of-building. Failure to comply with this restriction could cause harm to personnel or equipment.

Note:

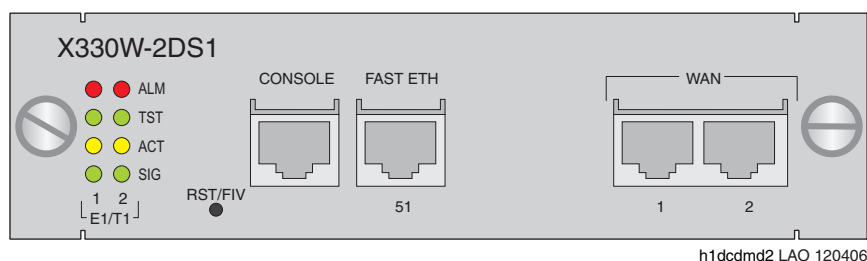
A shielded cable for the MM710 Media Module is required to meet emission requirements in European Union countries. The use of a shielded cable for the MM710 is preferred for installations worldwide.

The media modules enable the G700, with its primary controller, to host a variety of functions ranging from IP phones to traditional analog telephony ports. The media modules contain trunk or line interfaces and their associated circuitry. Each of the four media module slots has access to the 512-time-slot TDM bus, a 10/100 base T port, power (+5V, -48 V phantom) and ground. Each media module can be accessed and reset from the G700 Media Gateway Processor (MGP) or from the primary controller, and its status is indicated by an LED display.

What are data expansion modules

The G700 Media Gateway can accommodate any of the Avaya Data Expansion Modules. With expansion modules, customers can add additional LAN and WAN access modules directly to the G700.

Figure 4: Expansion Module (example)



Two expansion modules that the customer may purchase are:

- Avaya X330 WAN access routing module
- Avaya P330 LAN expansion module

What the Avaya X330 WAN access routing module provides

Customers with multiple branch offices need network solutions that are simple, flexible, and scalable. These customers may purchase the Avaya X330 WAN Access Routing Module as part of their configuration. This WAN Access Module provides WAN routing to the P330. The Avaya X330 WAN Access Routing Module also provides WAN access that can be used with external firewalls or VPN Gateways.

The Avaya X330 WAN Access Routing Module can be managed by three methods:

- Integrated Web-based management
- Avaya Network Management Console with VoIP SystemView
- Command Line Interface (CLI)

What the Avaya P330 LAN expansion module provides

Another Data Expansion that customers might purchase as part of their network is the Avaya P330 LAN Expansion Module. Features of this Data Expansion Module include:

- Maximum flexibility to the data stack
- Standard auto-negotiation
- Link Aggregation Group (LAG)
- LAG redundancy
- Link redundancy
- Congestion control
- 802.1Q/p VLAN priority



CAUTION:

Avaya Expansion Modules and Octaplane Stacking Modules are not hot-swappable. The G700 Media Gateway must be turned off before you remove or insert an Expansion Module. If there is an S8300 present that is also turned on, the S8300 should be shut down first, by pressing the Shutdown button until the OK to Remove LED shows a steady light.

What are stackable ethernet switches

The G700 Media Gateway can accommodate any of the Avaya stackable ethernet switches. With stackable ethernet switches, customers can add additional IP ports to the G700 in an octaplane stack of up to 10 units cabled together.

What the Avaya C360 stackable ethernet switch provides

The Avaya C360 family of stackable Ethernet workgroup switches includes:

- A range of modules with 24 or 48 10/100 Mbps ports and two 1-GB SFP slots for Gigabit Ethernet connections
- A Layer 3 capability

The available C360 switch models are as follows:

- C363T

This switch has 24 10/100 Mbps ports and two 1-Gigabit Ethernet ports. Maximum power consumption is 60 Watts.

- C363T-PWR

This switch has 24 10/100 Mbps ports with Power over Ethernet (PoE) and two 1-Gigabit Ethernet ports. Maximum power consumption is 420 Watts. Its power output per PoE port is 15.4 Watts.

- C364T

This switch has 48 10/100 Mbps ports and two 1-Gigabit Ethernet ports. Maximum power consumption is 90 Watts.

- C364T-PWR

This switch has 48 10/100 Mbps ports with Power over Ethernet (PoE) and two 1-Gigabit Ethernet ports. Maximum power consumption is 760 Watts. Its power output per PoE port is 15.4 Watts.

A C360 switch can co-reside in a stack with G700 Media Gateways. An Avaya C360 stack can contain up to 10 switches and up to three backup power supply units. The stacked switches connect using the Avaya X360STK stacking sub-modules that plug into a slot in the back of the Avaya C360. If the stack is split between two racks you can connect the C360s by using the X330SC or X330LC cables. The Avaya X330RC cable connects the top and bottom switches in the stack and provides redundancy and hot-swappability in the same way that modules can be swapped in a modular switching chassis.

Features of the C360 stackable ethernet switch include:

- You can connect up to 10 Avaya C360 switches in a stack.
Moreover, this stack can be either in one rack, split over several racks using the X330LC Long Cable, simply stacked without a rack.
- Avaya X360STK stacking sub-module that is used to connect Avaya C360 switches in a stack by way of the Octaplane.
- Avaya C360 BUPS back-up power supply module.

- One RJ45/RS232 front panel console connector that is used for both terminal and modem sessions.
- Three fan units with operation sensors for each switch.
- One virtual IP address for managing the whole stack that allows the C360 stack to be managed as a single entity.
- The ability to hot-swap one switch at a time by activation of the redundant cable:
 - Does not disrupt the operation of other Avaya C360 switches.
 - Does not change stack configuration.
 - Does not require network downtime.
- Connection through Telnet from the front panel ports of any switch:
 - Multiple levels of password protection
 - Login and inactivity timeouts

Building a stack

Follow the guidelines in this section in order to build a working stack certified using any combination of the following devices:

- P330 series
 - P330-ML series
 - G700
 - C360 series
1. Add only a single box at a time to an existing stack.



Important:

The stack master (also called "stack IP Agent") may fail to preserve existing "stack configuration" if you will add more than a single device to an existing stack at a time.

- After adding the first box, wait until the stack is functioning fully before adding the next device.
2. Refer to [Table 5](#) to see which firmware versions can be used in mixed stacks. For example, if you wish to add a P332G-ML to a stack with C360 4.5 switches, the P332G-ML switch must have firmware version 4.5.8.
 - Upgrade/downgrade the firmware of switches that do not match version in the table.



Tip:

It is highly recommended to upgrade/downgrade before connecting the added box to an existing stack.

- Ensure switches of the same type have the same firmware version

Table 5: Firmware Versions Matrix

	Required version						
	Stack without C360					Stack with C360	
Switch	3.11	3.12	4.0	4.1	4.5	4.3	4.5 or higher
P333T	3.11.0	3.12.1	4.0.17	4.1.6	4.1.6	N/A	N/A
P334T	3.11.0	3.12.1	4.0.17	4.1.6	4.1.6	N/A	N/A
P333R	3.11.0	3.12.0	4.0.9	4.1.5	4.1.5	N/A	N/A
P333R-LB	3.11.0	3.12.3	4.0.6	4.1.5	4.1.5	N/A	N/A
P332MF	3.11.0	3.12.1	4.0.17	4.1.6	4.1.6	N/A	N/A
P333T-PWR	3.11.0	3.12.1	4.0.17	4.1.6	4.1.6	N/A	4.1.6
G700	3.11.0	3.12.1	4.0.17	4.1.6	4.1.6	N/A	4.1.6
P334T-ML	3.11.16	3.11.16	4.0.15	4.1.3	4.5.8	N/A	N/A
P332G-ML	3.11.15	3.11.15	4.0.15	4.1.3	4.5.8	N/A	4.5.8
P332GT-ML	3.11.15	3.11.15	4.0.15	4.1.3	4.5.8	N/A	4.5.8
C363T	N/A	N/A	N/A	N/A	N/A	4.3.12	4.5.14
C346T	N/A	N/A	N/A	N/A	N/A	4.3.12	4.5.14
C363T-PWR	N/A	N/A	N/A	N/A	N/A	4.3.12	4.5.14
C364T-PWR	N/A	N/A	N/A	N/A	N/A	4.3.12	4.5.14

Note:

Position the C360 switches either at the top or bottom of the stack to ensure mechanical stability.

Stack Master election rules

[Table 6](#) lists the switches in order of election priority from highest to lowest.

Note:

If there are two switches with the same firmware version and the same election priority, the switch positioned lower in the stack becomes Stack Master.

Table 6: Stack Master election priority

Switch type	Switch mode	Stack Master election priority
C363T, C363T-PWR	Layer 2	1
C364T, C364T-PWR	Layer 2	2
C363T, C363T-PWR	Layer 3	3
C364T, C364T-PWR	Layer 3	4
P332GT-ML	Layer 2	5
P332G-ML	Layer 2	6
P334T-ML	Layer 2	7
P332GT-ML	Layer 3	8
P332G-ML	Layer 3	9
P334T-ML	Layer 3	10
G700	N/A	11
P333R, P333R-LB	Layer 2	12
P333T, P334T, P332MF	N/A	12
P333T-PWR	N/A	13
P333R, P333R-LB	Layer 3	14
P333R-LB	Webswitch	15

What are the functions of the S8300 LED Indicators

A set of LED indicators the faceplate of the S8300 are separate from those of the G700. A shutdown button is also on the faceplate, which when depressed for about three seconds, will shut down the system, including the operating software on the S8300. The LED flashes when shutdown is in progress and remains on steady when it is safe to remove the S8300 or to power down.

The functions of the S8300 LEDs are:

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

Note:

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

- The green APP (S8300C) or TST (S8300B) LED on the S8300 (primary controller or LSP) is on when Communication Manager is running.
- The yellow ACT LED on the S8300 is on whenever a G700, an IP telephone, or an IP console is registered with the S8300. It is off when none of these IP endpoints are registered.
- The green OK-to-Remove LED on the S8300 indicates that shutdown is complete and that it is safe to remove the server or power down the system.

When the S8300 is a local survivable processor (LSP), no LEDs will be lit during normal operations. In case of a network failure or loss of contact with the primary S8300 (or S8500 or S8700/S8710), the G700 Media Gateway will register with the LSP. At that time, the red Alarm LED will light.

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

Media servers supporting the G700 media gateway

Each G700 is associated with a primary call controller. The primary controller may be an S8300, S8500, or S8700/S8710 Media Server. The S8300 is on a circuit pack that is always installed in slot V1 of a G700. The S8500 or S8700/S8710 is housed in a separate box that connects to the G700 over a network through a C-LAN circuit pack. Both media servers can support multiple G700s.

The S8300 Media Servers can be configured as either a primary server or a Local Survivable Processors (LSP). The G700 with a media server supports the entire range of adjuncts and peripheral equipment supported by Communication Manager.

Figure 5: Avaya S8300 Media Server (S8300C shown)



What is the S8300 media server

The S8300 Media Server is an Intel processor complex that mounts in the first media module slot (V1) of the G700 Media Gateway. The S8300 Media Server has:

- Avaya Communication Manager (For a full description see: <http://www.avaya.com/support>)
- Administration and maintenance provisioning software
- **(S8300B model only)** 20 GB or 30 GB hard drive
(S8300C model only) 40 GB hard drive
- **(S8300B model only)** 512 MB RAM (in two 256 MB DIMM strips)
(S8300C model only) 1 GB RAM (with one 1 GB DIMM)
- Web server
- Linux OS (Red Hat)
- Support of H.248 and H.323 Protocols
- TFTP server and other IP services
- **(S8300C model only)** Internal compact flash drive, which is used as the primary reboot device and provides additional reliability with the RAMdisk and hard drive

Note:

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

What is a Local Survivable Processor (LSP)

The S8300 Media Server can act as a survivable call-processing server for remote or branch customer locations. As an LSP, the S8300 Media Server carries a complete set of Communication Manager features, and its license file allows it to function as a survivable call processor. If the link between the remote G700 Media Gateways and the primary controller is broken, those telephones and G700s that are designated to receive backup service from the LSP will register with the LSP. The LSP will provide control to those registered devices in a license error mode (see *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207).

Primary controller and LSP in the same stack

You can install an LSP in the same stack as that of the S8300 primary controller. In this case, the primary controller and LSP are in separate G700 Media Gateways. Their respective G700 Media Gateways can share the same Octaplane cabling, such that the LSP can register and communicate with the primary controller. In addition, the LSP is accessible and can access the LAN through the Octaplane connection. The LSP does not require a separately-cabled Ethernet connection. A separate Ethernet connection to the LSP, however, is optional.

What is the S8400 media server

The G700 Media Gateway can be controlled by an external S8400 Media Server. The S8400 is connected to the G700 over the network through a C-LAN circuit pack in the G600 or G650 Media Gateway. The S8400 can also be connected to the G700 over the network directly to either of two Ethernet ports on the S8400, depending on which is configured in the software as the processor Ethernet port.

What is the S8500 media server

The G700 Media Gateway can be controlled by an external S8500 Media Server. The S8500 is connected to the G700 over the network through a C-LAN circuit pack in the G600, SCC1, or MCC1. The S8500 can also be connected to the G700 over the network directly to either of two Ethernet ports on the S8500, depending on which is configured in the software as the processor Ethernet port.

What is the S8700/S8710/S8720 media server

The G700 Media Gateway can be controlled by an external S8700/S8710/S8720 Media Server (sometimes referred to as an ECC configuration). The S8700/S8710/S8720 with the G600, G650, SCC1, and/or the MCC1 Media Gateways can control the G700. The S8700/S8710/S8720 is connected to the G700 over the network through a C-LAN circuit pack in the G600, G650, SCC1, or MCC1.

Note:

The S8700 Media Server is no longer available for new installations.

Information on installing the G700 using the S8400, S8500 or S8700/S8710/S8720 as the primary controller can be found in Chapters 4 and 6 in this book.

About endpoint and adjunct components

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

Other components and adjunct systems that make up the S8300 Media Server with a G700 Media Gateway include:

- Analog phones and fax machines
- DCP phones
- IP phones
- IP Softphones
- LAN Ethernet switches
- Avaya Integrated Management
- INTUITY AUDIX LX Messaging System
- IA 770 INTUITY AUDIX Messaging Application
- ASAI Co-Resident DEFINITY LAN Gateway (DLG)
- Call Center
- Uninterruptible Power Supply (UPS)
- Universal Serial Bus (USB) Modems
- USB Compact Flash device (S8300C only)
- DVD/CD-ROM drive

See [Chapter 7: Telephones and adjunct systems](#) for more information on installing adjuncts.

About installation planning

In the following sections of this installation guide, you will be guided through the installation of several configurations. Before the G700 components are physically installed on the customer's site, several steps will already have been completed to assure that the actual installation will go smoothly:

- Sales personnel have verified that the product is suited to the customer's application.
- Planning and implementation personnel have conducted preliminary inspections of the site and of the other equipment to assure that the S8300/G700 solution will operate at its full potential.

- A data network readiness assessment has been completed to assure that the solution will function optimally within the customer's network.

Each of these processes have been documented before the installation. You should verify that you have all the necessary information before going to the site (see [Appendix B: Information checklists](#)).

What the planning documentation provides

To guide you in your preparations for the installation, use the Installer's Checklists (see [Appendix B: Information checklists](#)) to verify that you have the tools, software, and information that you need to install the G700.

The planning documentation will provide you with information about:

- What equipment you will be installing
- What kind of system you will be integrating
- Whom to contact on site about delivery, system questions, or network concerns
- Whom to contact at your home office in case of questions
- Whether you need a special pass or an escort
- How to gain entrance to the installation location if it is locked
- Where to install equipment
- Where to find a telephone near the installation location

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

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

As a first-time user:

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

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

What site verification does

A pre-installation site inspection allows you to verify that the site requirements have been met for adequate environmental conditions, power and grounding availability, safety, and security conditions. If you find discrepancies between the specifications necessary for proper installation of equipment and the conditions on site, contact your Project Manager before proceeding with the installation.

What network integration requires

Integration into the customer's network will require coordination with the network manager and the planning and implementation personnel. They will ascertain the customer's need for DHCP service and the intended network configuration and applications. In addition, Avaya offers Network Readiness services to assist in evaluating and preparing the network for all configurations.

The Project Manager will provide information to be used by the installers. The documentation must include dial plans and other telephony information, as well as IP addresses, IP masks, and other network information. This information will be specific to each customer. To install the solution in an efficient manner, you must collect and organize this information before going to the site.

Reviewing demarcation points and connectivity for the IA770 INTUITY AUDIX Messaging Application

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

The demarcation point for the Avaya IA 770 INTUITY AUDIX Messaging Application is the S8300 Media Server ethernet ports. The customer is responsible for ensuring that the following items are correct and functioning normally:

- The LAN cable and connector used to connect to the S8300 Media Server.
- LAN administration outside of the Avaya equipment.
- Maintaining the TCP/IP addresses and administration on the S8300 Media Server after installation, unless otherwise specified by contract
- Valid IP address, subnet mask, and gateway information for administration on the S8300 Media Server

Avaya service technicians who are dispatched for IA 770 system installation are not responsible for troubleshooting the LAN.

Maintaining system security

Remember that security is important.

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

- Change the passwords for the system administrator (sa), voice mail administrator (vm), and dadmin logins before you begin the verification and acceptance of the IA 770 software.
- Do not leave written passwords in a place where they are accessible by others.
- At the first opportunity, privately give the passwords to the customer's designated representative.
- If you suspect that the security of any password has been compromised, immediately notify your project manager or system administrator.

Verifying features for the IA770 INTUITY AUDIX Messaging Application

In order to use IA 770 INTUITY AUDIX, you must verify with an account representative that the following Avaya Communication Manager features have been enabled in the license file:

- Maximum Administered IP Trunks - This number must be equal to or greater than the number of IP trunk ports used by IA 770.
- ARS
- ARS/AAR Partitioning
- ISDN-PRI
- H.323 Trunks (IP Trunks)
- Private Networking
- Uniform Dialing Plan
- Basic Call Setup
- Basic Supplementary Services
- Supplementary Services with Rerouting
- Transfer into QSIG Voice Mail
- Value-Added (VALU)

About installation and cabling

The Avaya G700 Media Gateways can be installed in a variety of configurations:

- As a standalone unit with one G700
- With multiple G700 Media Gateways in a stack
- In combinations of Media Gateways and Avaya C360 family devices (see [Building a stack](#) on page 75).

Up to ten G700 Media Gateways and/or Avaya C360 devices can be combined in a single stack. The G700s can be controlled by an Avaya S8300, S8400, S8500, or S8700/S8710 Media Server.

In a typical installation, you arrive at the site equipped with all the tools and information needed to install a G700 and, possibly, an S8300.

In this section, you complete the following procedures:

- [Verifying the on-site checklist](#) on page 85
- [Verifying Environmental conditions](#) on page 86
- [Unpacking and checking the order](#) on page 87
- [Installing the G700 media gateway](#) on page 87
- [Cabling multiple units](#) on page 98
- [Attaching Ground Conductors](#) on page 102

Note:

When installing a G700, complete all tasks in this chapter to install the gateway before doing the media server administration (for example, `add media-gateway`).

Verifying the on-site checklist

When you reach the customer's site, verify each item on the Installer's Checklist (see [Appendix B: Information checklists](#).)



Tip:

It is recommended that you consult with the customer network manager for IP and DNS addressing, as well as for testing the installation.

Also, before proceeding with the installation, you should verify that the proper environmental and safety conditions exist.

Verifying Environmental conditions

Verify that temperatures and clearances are within the recommended technical parameters. Consult the table of Technical Specifications in [Appendix A: Technical information](#).



CAUTION:

Verify that temperature and clearance ranges are within tolerable limits. The thermal sensors may shut down equipment if it is subjected to conditions beyond the recommended limits. Equipment can be damaged if these restrictions are not respected.

Power Verification

Check that an adequate number of power outlets are available. Verify that the G700 Media Gateways and the other equipment in the rack do not present a possible overcurrent or overload to the customer's branch circuit and/or power distribution strip. Power requirements are listed in [Appendix A: Technical information](#).



WARNING:

Do not overload the power circuit.

Grounding Verification

Ensure that the installation site has access to approved grounds and that either a trained technician or a licensed electrician will be verifying all grounds and installing the Supplementary Ground Conductor (consult [Attaching Ground Conductors](#)).



WARNING:

Installation in a Restricted Access Location and secure access are required in Finland and Norway.

The G700 Media Gateway relies on two ground connections (mains plug with an earth contact and a permanent Supplementary Ground Conductor). Because of unreliable earthing concerns in Finland and Norway, the G700 Media Gateway must be installed in a Restricted Access Location (RAL). An RAL is defined as an access that can be gained only by trained service personnel or customers who have been instructed about the reasons for the restricted access and any safety precautions that must be taken. In these cases, access to the G700 Media Gateway is gained by the use of a tool (such as a lock and key) or other means of security.

If you have any questions about the safety conditions, contact your Project Manager. When you have verified that the site is ready for a safe installation, proceed with the installation.

Unpacking and checking the order

Cross-check your customer's order with the planning documentation you have been given. media modules, telephones and other equipment are listed on your planning and shipping documentation. Placement for the media modules and other equipment are indicated, as well.

Verify that all necessary elements have been received and are in good condition. If there are missing or damaged elements, contact the Project Manager for instructions. The planning documentation will list contact information for the Project Manager and other key personnel.

**CAUTION:**

Wear an anti-static wrist ground strap whenever handling components of an Avaya G700 Media Gateway. Connect the strap to an approved ground, such as an unpainted metal surface.

If you have any questions about the equipment order, or if the equipment has been damaged, contact your Project Manager. When you have verified that the order is complete and that you have all of the necessary components and tools, proceed with the installation.

Installing the G700 media gateway

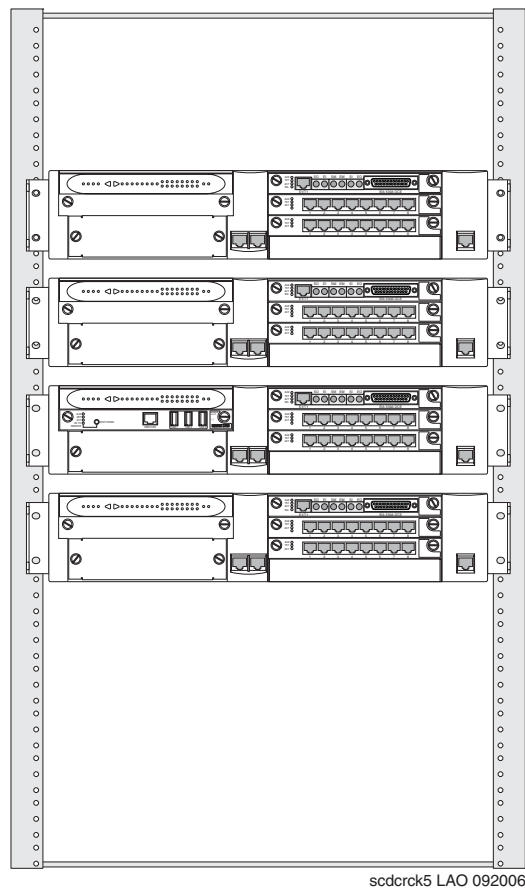
After you have verified the site conditions and the shipment, you proceed with the installation of the hardware.

Perform the following steps:

- [Preparing the G700 media gateway](#) on page 88
- [Mounting the G700 media gateway in the rack](#) on page 89

[Figure 6: Avaya G700 Media Gateways](#) on page 88 shows a stack of four G700 Media Gateways installed in a rack-mounted configuration. Of the four G700s, only one contains an S8300 Media Server in slot V1 (second up from the bottom).

Figure 6: Avaya G700 Media Gateways



Preparing the G700 media gateway

The instructions that follow guide you through a process of preparing the Avaya G700 Media Gateway after you have mounted the empty chassis in the rack. It is possible to equip an empty G700 chassis before positioning it in the rack. If you are working where space is limited, you may wish to prepare the G700 before rack insertion.



CAUTION:

When handling any components of an S8300 Media Server with G700 Media Gateways, wear an anti-static wrist ground strap. Connect the strap to an approved ground such as an unpainted metal surface.

The G700 can stand on a flat surface or be mounted in the standard 19-inch rack. If the G700 is to be mounted in a rack, you have the choice of fastening the unit to the rack either at the front of the unit or at the middle. This positioning choice will depend on space arrangements. In either case, mounting brackets must be attached to the sides of the chassis, either at the center or to the front of the chassis.

To affix mounting brackets to the G700

1. Remove the screws from the bracket kit.
2. Position a bracket over the desired mounting position.
3. Affix the bracket to the chassis with the screws provided.
4. Tighten with the screwdriver.
5. Repeat on the other side.

If the G700 is to be a table-top unit, four feet must be attached to the bottom of the unit. Use the following procedure to do this:

To affix feet on the table-top G700

Note:

Use this procedure only if the G700 will be installed as a table-top unit (not in a data rack).

1. Remove the four feet from their packaging.
2. Turn the G700 Media Gateway over to allow the feet to be mounted.
3. Position one foot into the mounting site near the corner of the chassis.
4. Press the plastic rivet into the foot with a stylus until it is firmly seated on the chassis.

You have now prepared the G700 Media Gateway for mounting, and, assuming you are going to use a data rack, you are ready to mount the chassis in the rack.

Mounting the G700 media gateway in the rack

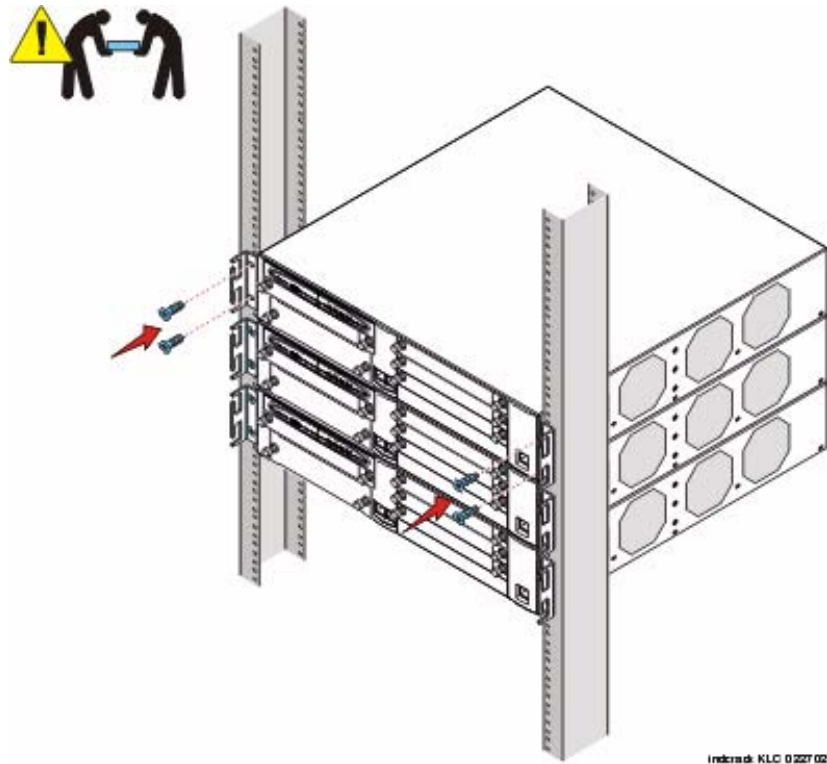
The G700 Media Gateway mounts in a standard 19-inch rack. It is held in place by screws through the two mounting ears. The unit can be mounted either in the center of the unit or at the front of the unit; however, only the front mount allows use of the guides for electrical cables. To avoid balancing problems and cabling complications, the racks should be filled from the bottom; that is, mount units in the lower positions first.

Before mounting the G700, check for the following:

- Ensure that the rack is bolted to the floor and is earthquake-protected, if required. If the rack is not securely fixed in place, do not proceed with the installation.
- If the G700 is being mounted in a rack with other equipment already installed, the G700 must be positioned to avoid imbalance.

- The G700 is shipped with 3 sets of four mounting screws. Choose the set of screws that match the screw holes in the rack being used.
- The G700 weighs 22.5 pounds (10 kg) empty and between 27 and 34 pounds (between 12 and 16 kg) when equipped with media modules. Two people may be needed to mount the G700 Media Gateway in the rack.

Figure 7: Rack Mounting



To mount the G700 media gateway in the rack

1. Position the G700 in the rack.
Assure that there is adequate ventilation.
2. Verify that the screw holes are aligned with the rack hole positions.
3. Insert the mounting screws.
Use two screws on each side.
4. Tighten the mounting screws.
Avoid overtightening.
5. Verify that ventilation vents are not obstructed.
6. Repeat to add other G700 media gateways to the rack, as described in the planning documents.

If you are installing multiple G700s, continue building the stack. Up to 10 units can be linked together ([Figure 14: Cabling Multiple Units in a Single Rack](#) on page 99); these may be G700s or Avaya C360 family switches.

At this point, you have mounted the G700 chassis in the rack and are ready to insert S8300 Media Servers and media modules as required in the planning documentation.

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

The S8300 Media Server is inserted into the G700 Media Gateway slot #1 (v1), whether it is the primary server or configured as a Local Survivable Processor (LSP). The S8300 can only be inserted in the slot (v1) on the left side of the G700 Media Gateway. For the S8300B only, the LED module must be pulled from the G700 chassis to provide clearance for the S8300 Media Server.

 CAUTION:

If you are removing an S8300, use the shutdown button to stop the operating system (press and hold for 2-3 seconds). The OK to Remove LED will flash while the shutdown is in progress and will turn steady green when it is safe to remove the S8300.

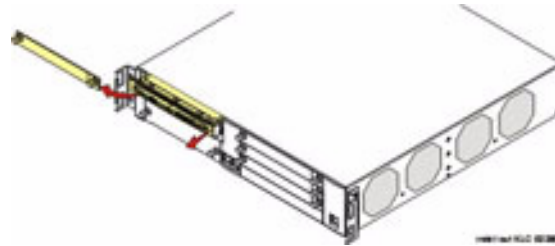
Note:

A G700 Media Gateway stack can contain more than one S8300 Media Server. In this case, one S8300 Media serves as the primary controller and the other S8300 Media Server serves as an LSP. The LSP then uses the Octaplane connection of its housing G700 Media Gateway for LAN accessibility.

To insert the S8300 into slot #1 of the G700 media gateway

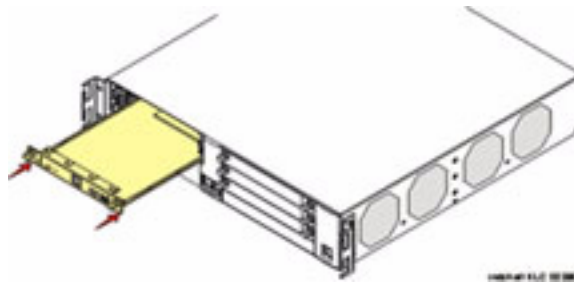
1. Clear the left side of the G700 Media Gateway.
 - a. Remove the blank plate from slot #1.
 - b. If the model is an S8300B, disengage the LED module and remove it from the G700 Media Gateway.
2. Line up the Avaya S8300 Media Server module squarely with its bay opening.

Figure 8: Clear the left side of the G700 Media Gateway



-
3. Engage both sides of the S8300 Media Server module in the interior guides and guide the module halfway into the chassis.

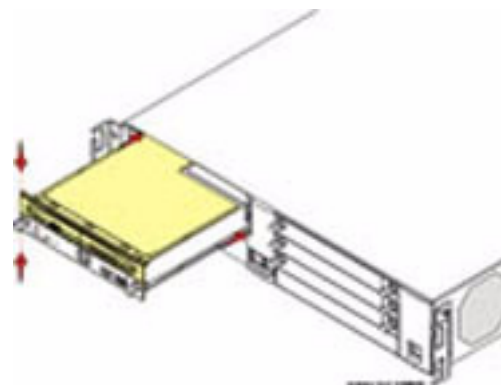
Figure 9: Insert S8300



-
4. For an S8300B only, align the LED module in its guides and gently push it into place, keeping the LED module safely within its guides and maintaining an even pressure to assure that the module does not become twisted or disengage from the guides.

Guide the longer, left side of the LED module into the chassis until the shorter, right edge of the module can engage in its guides.

Figure 10: Align the LED module and the S8300 Media Server



5. For an S8300B, push steadily and firmly until the faceplates of the S8300 Media Server and the LED module are even and then push the two units into the housing together.

For an S8300C, push steadily until the faceplate of the S8300 Media Server is even with the LED module faceplate.

6. Apply firm pressure to engage the connectors.

The connector has different length pins. The long pins will engage first to provide grounding. Medium length and short pins will provide power and signal.

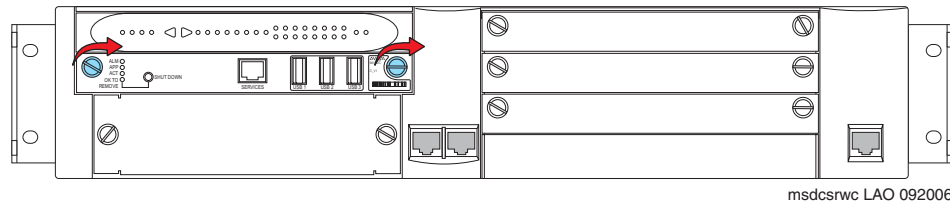
7. Tighten the captive screws on the S8300 Media Server module.



WARNING:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Figure 11: Tighten screws



msdcsrcw LAO 092006

Inserting media modules

Following the planning documentation, you can insert the required media modules into their designated bays. The G700 Media Gateway can accommodate up to four media modules, or plug-in circuit packs. The choice of media modules is dictated by the offer selected by the customer and the configuration of the system.

Consult the planning documentation and the order form to determine which modules you will be installing. The planning documents also indicate into which slots the modules are to be inserted. The media modules available at this time are:

- Avaya MM710 T1/E1 Media Module
- Avaya MM760 VoIP Media Module (support G.723, G.726, and G.729)
- Avaya MM711 Analog Media Module (8 ports, stations or trunks)
- Avaya MM714 Analog Media Module (4 station ports and 4 trunk ports)

Note:

Analog DID trunk connections are to be associated with the ports labeled "Line" and not "Trunk".

- Avaya MM712 8-port DCP Media Module
- Avaya MM716 24-port Analog Media Module
- Avaya MM717 24-port DCP Media Module (Install no more than 3 in a single G700. The ports must be used in-building only)
- Avaya MM720 8-port BRI Media Module (for trunks or stations)
- Avaya MM722 2-port BRI Media Module

For detailed descriptions of the media modules see *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207.



WARNING:

The Avaya G700 media gateway must not be operated with any slots open. Failure to cover empty slots with the supplied blank plates can cause overheating due to inadequate air distribution.



CAUTION:

A maximum of 3 MM717 24-port DCP Media Modules can be installed in a single G700. Also, the ports on the MM712 and MM717 are intended for in-building use only. Phone lines connected to those ports are not to be routed out-of-building. Failure to comply with this restriction could cause harm to personnel or equipment.



CAUTION:

The connector pins can be bent or damaged if the module is handled roughly, or if misaligned and then forced into position.

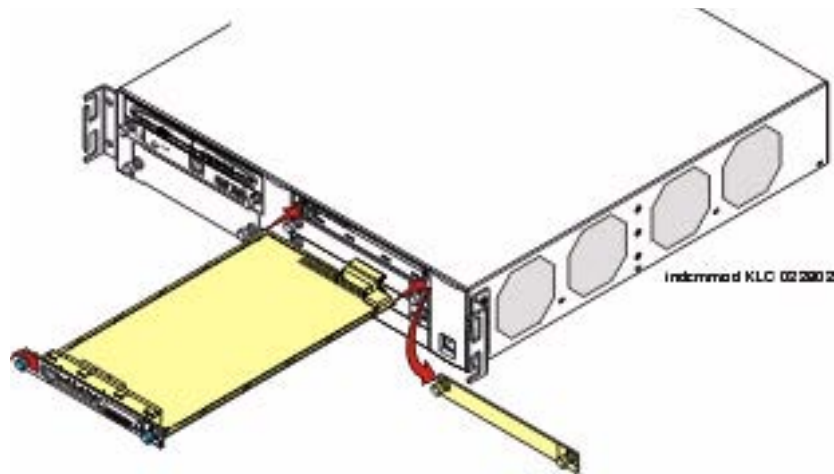


CAUTION:

Separate ESD paths to the chassis ground connect to the media modules at the spring-loaded captive screws. Use a screw driver to ensure the captive screws are securely tightened to prevent damage to the equipment.

To insert media modules

1. Remove the blank plate from the empty bay.
2. Position the media module squarely before the selected bay on the front of the G700 Media Gateway chassis and engage both sides of the module in the interior guides.
3. Slide the module slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengaged from the guides.

Figure 12: Insert Media Module

-
4. Apply firm pressure to engage the connectors.

The media module connector has different length pins. The long pins will engage first to provide grounding. Medium length and short pins will provide power and signal.

5. Lock the media module into the chassis by tightening the spring-loaded captive screws on the front of the module.

**WARNING:**

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

**WARNING:**

After you have connected telephones to the various media modules, be sure to add circuit protection to the lines (see [Complete the telephone installation process](#) on page 340).

At this point, you have readied the G700, inserted the S8300, if required, and inserted the media modules, as described in the planning documentation. Next, if required, the Expansion Module should be inserted into its bay.

Inserting an Expansion Module

The Expansion Modules provide increased networking and connectivity capabilities. These modules may be mounted on the G700 Media Gateway in the slot on the lower left side of the unit below slot V1 (see [G700 media gateway with an S8300 media server: front view](#) on page 70).

 CAUTION:

The Expansion Module is not hot-swappable. That is, the G700 must be powered off before you insert or remove an Expansion Module. If there is an active S8300 present, the S8300 should be shut down by pressing and holding the Shutdown button for 2-3 seconds. The OK to remove LED will flash during shutdown and turn on steady when it is safe to power down.

To insert an Expansion Module into the G700 media gateway

 CAUTION:

Turn off the power to the unit if the equipment has been in operation.

1. Remove the blank plate covering the bay.
2. Align the printed circuit board with the interior guide rails.

Note:

The printed circuit board fits into the guide rail. The metal base plate does not.

3. Firmly press the Expansion Module into the G700 Media Gateway until it is completely inserted.
4. Tighten the two screws on the front panel of the Expansion Module.

 WARNING:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

 WARNING:

The Avaya G700 Media Gateway must not be operated with any slot open. Empty slots must be covered with the supplied blank plates.

At this point, you have readied the G700, inserted the S8300, if required, inserted the media modules and the Expansion Module, as required in the planning documents. If more than one unit (G700 and/or Level 2 switches and routers) will be connected in the configuration you are installing, the next step will be to insert an Avaya X330STK Stacking Sub-Module.

Inserting an Avaya X330STK Stacking Module

G700 Media Gateways can be mounted in equipment stacks with routers, switches, or other G700s. The stack is limited to ten elements. To link multiple units, each G700 must be equipped with an Avaya X330STK Stacking Module, which is mounted through the rear panel (back view) of the G700.

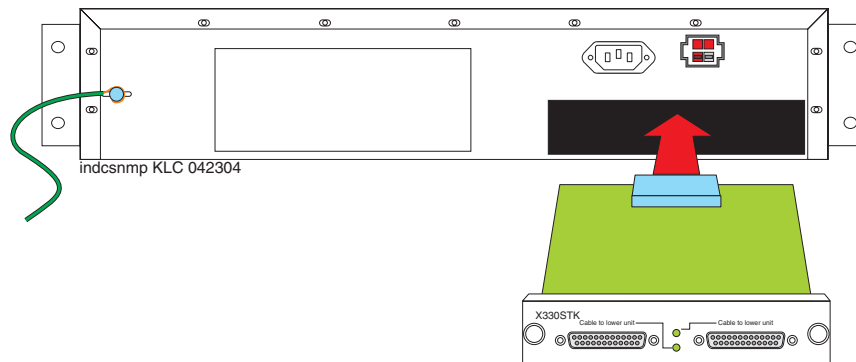
⚠ CAUTION:

The Stacking Sub-Module is not hot-swappable. That is, the G700 must be powered off before you insert or remove a Stacking Module. If there is an active S8300 present, the S8300 should be shut down by pressing the Shutdown button. Hold the button in 2–3 seconds until the OK to Remove LED starts flashing. When the LED turns on steady, power can be safely turned off.

To insert an Avaya X330STK Stacking Module

1. Remove the blank plate from the back of the G700.
2. Insert the Avaya X330STK Stacking Module gently in the bay in the back of the G700, ensuring that the metal base plate is aligned with the guide rails.

Figure 13: Insert Stacking Module in G700 (back view)



3. Press the Avaya X330STK Stacking Module in firmly until the connector at the back of the module is completely inserted into the internal connector on the G700.
4. Tighten the screws on either side of the module.

At this point, the required modules and cabling units have been inserted into the G700 Media Gateway. The next step will be to install cabling.

Cabling multiple units

Avaya G700 Media Gateways can be mounted in equipment stacks with routers, switches, or other Media Gateways. These elements are all compatible and are installed similarly. Consult Avaya P333T User Guide for installation and cabling information. To link multiple units, each G700 Media Gateway must be equipped with an Avaya X330STK Stacking Module on the rear panel. Then, each unit in the stack is linked to the one above it. Finally, the bottom unit is linked to the top unit. Stacks should always be built from the bottom, and new units should be added at the top. Up to 10 units can be stacked in this way.

When deciding where to position the unit, ensure that:

- It is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines and fluorescent lighting fixtures.
- Water or moisture cannot enter the case of the unit.
- There is a free flow of air around the unit and the vents in the sides of the case are not blocked.

The two ends of the Octaplane cables incorporate different connectors. Each connector can only be connected to its matching interface.

The following cables are used to connect stacked units:

- Short Octaplane cable (Avaya X330SC) - light, ivory-colored cable used to connect adjacent units.
- Long Octaplane and Extra-Long Octaplane cables (Avaya X330LC/X330L-LC) - light, ivory-colored cable used to connect units from two different physical stacks or those separated by more than 12 inches (30 cm).
- Redundant and Long Redundant cables (Avaya X330RC/X330L-RC) - black cable used to connect the top and bottom switches of a stack.

Figure 14: Cabling Multiple Units in a Single Rack

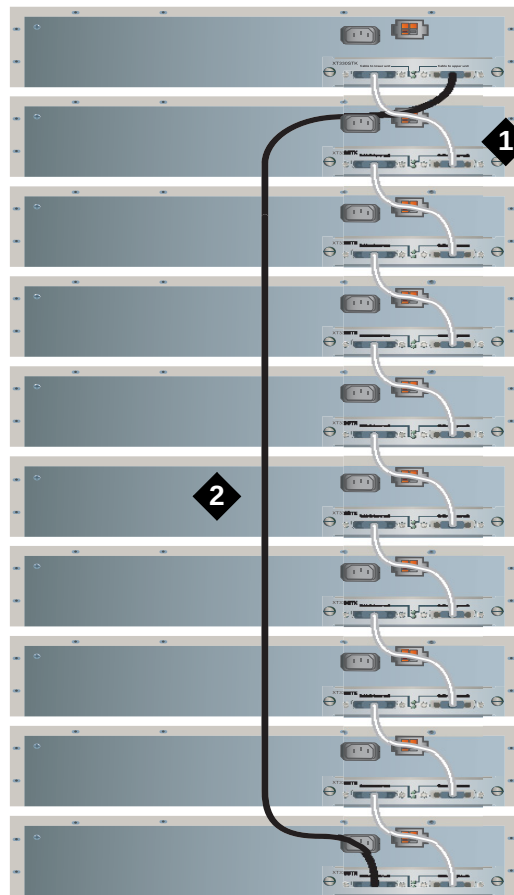


Figure notes:

- 1. Short Octaplane cable (X330SC)**
- 2. Redundancy cable (X330RC)**

To connect units within a single stack

1. Connect the light grey connector of the short Avaya X330SC cable (12 in, 30 cm) to the port marked “to upper unit” in the bottom-most stack element.
2. Connect the dark grey connector of the same short X330SC cable to the port marked “to the lower unit” in the unit above.
3. Repeat until you reach the top element in the stack.

Up to ten G700s and/or other Cajun devices can be stacked together.

To implement stack redundancy:

4. Use the Redundant Cable to connect the port marked “to lower unit” on the bottom element to the port marked “to upper unit” on the top element of the stack.

If you have elements of a stack in two racks, you must use the Avaya X330LC cable to connect them. You may not link more than 10 units to form a stack, but those units can be mounted in more than one rack.

To link elements in multiple racks

1. Use the long (6ft, 2 m) Avaya X330LC cable to connect elements in two racks.
2. Connect the Avaya X330LC cable (dark grey connector) to the port on first unit of the stack marked “to the lower unit.”
3. Connect the Avaya X330LC cable (light grey connector) to the port on the last unit in the stack marked “to the upper unit.”

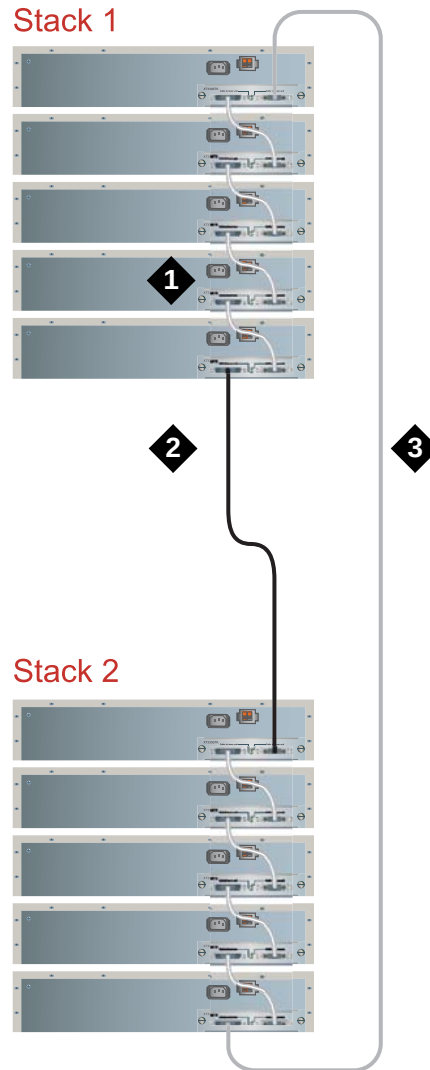
To implement stack redundancy:

4. Connect the dark grey connector of the black Redundancy Cable (X330RC) to the port marked “to lower unit” on the bottom unit of the stack.
5. Connect the light grey connector of the black Redundancy Cable to the port marked “to upper unit” on top unit of the stack.



CAUTION:

Do not cross-connect two stack elements with two Octaplane (light-colored) cables. If you wish to cross-connect for redundancy, use a black redundancy cable.

Figure 15: Linking Units in Multiple Racks**Figure notes:**

1. Short Octaplane cable (X330SC)
2. Redundancy cable (X330RC)
3. Long cable (X330LC)

You have now mounted the fully equipped Avaya G700 Media Gateway in the rack, and cabled units together as described in the planning documents. When all the units are mounted, and cabled, you are ready to connect to electrical ground conductors.

Attaching Ground Conductors

To assure safe installation and operation, carefully read all requirements, recommendations and instructions. Pay special attention to all CAUTION, WARNING, and DANGER statements.



WARNING:

Make sure that the G700 has a reliable earth ground connection, whether it is connected directly to a branch circuit or to a power distribution strip.



WARNING:

Installation in a Restricted Access Location and secure access are required in Finland and Norway.



CAUTION:

System grounding must comply with the general rules for grounding provided in Article 250 of the National Electrical Code (NEC), National Fire Protection Agency (NFPA) 70, or the applicable electrical code in the country of installation.

What are general grounding requirements

For AC Input: - Two safety grounds are required to ensure safe operation of the G700 Media Gateway:

- Ground conductor — part of the AC power cord
- Field-installed green/yellow conductor, referred to as the Supplementary Ground Conductor

Both safety grounds must be connected to an approved ground. If a power cord accompanies the G700, use that cord whenever possible.

For DC Input: - The +48Vdc lead provided for DC power input to the G700 Media Gateway must be grounded at the source to an approved ground. The -48Vdc is the active lead. Both leads must be floating at the input to the G700. In addition, the Supplementary Ground Conductor must be installed on the G700 and connected to an approved ground.

The customer must select a location for the G700 Media Gateway installation that is no more than 25 feet (7.6 m) from an approved ground. If this location requirement is not met, the customer must contact a licensed electrician to install a Supplementary Ground Conductor per Article 250 of the National Electrical Code (NEC).



WARNING:

If the installation location is greater than 25 feet (7.6 m) from an approved ground, do not install the Avaya G700 Media Gateway until a licensed electrician is present to install a Supplementary Ground Conductor.

A 25 foot (7.6 m) Supplementary Ground Conductor is provided with the equipment, and is constructed of 10 AWG (4.0 mm²) wire, with an insulated ring terminal crimped to one end that is suitable for the #8 (M4) stud/screw on the rear of the G700 chassis.

The customer will need to provide a means of connecting this Supplementary Ground Conductor to an approved ground according to Article 250 of the National Electrical Code (NEC).

A ground block is available for use when multiple G700 Media Gateways are being installed. The ground block, intended for rack mounting, has ten terminals available for terminating Supplementary Ground Conductors. Up to ten G700 Media Gateways can be grounded at the block installed close to the equipment (on a rack) and then a single ground conductor can be routed from the same block to an approved ground. If the ground block is to be used, it must be ordered separately.



DANGER:

Failure to install both grounds will void the Product Safety certifications (UL and the CE Mark) on the product, as well as allow a hazard to be present that could result in death or severe personal injury.

Because of unreliable earthing concerns in Finland and Norway, the G700 Media Gateway must be installed in a restricted access location. A restricted access location is defined as access that can be gained by only Service Personnel or Customers who have been instructed about the reasons for the restricted access and any safety precautions that must be taken. In these cases, access to the G700 Media Gateway is gained by the use of a tool (such as a lock and key) or other means of security.



WARNING:

For Installations in Finland and Norway, the Avaya G700 Media Gateway relies on two ground connections (mains plug with an earth contact, and a Supplementary Ground Conductor).

What are approved grounds

An approved ground is the closest acceptable medium for grounding the building entrance protector, entrance cable shield, or a single-point ground of electronic telephony equipment. If more than one type of approved ground is available on the premises, the grounds must be bonded together as required in Section 250-81 of the NEC for the US or per the local electrical code regulations in the country of installation.

Approved grounds can be any of the following options:

- **Grounded building steel**

The metal frame of the building, where it is effectively grounded by one of the following grounds:

- Acceptable metallic water pipe
- Concrete encased ground
- Ground ring

● Acceptable water pipe

A metal underground water pipe, at least 1/2-in. (1.3 cm) in diameter, in direct contact with the earth for at least 10 ft. (3m). The pipe must be electrically continuous (or made electrically continuous by bonding around insulated joints, plastic pipe, or plastic water meters) to the point where the protector ground wire connects. A metallic underground water pipe must be supplemented by the metal frame of the building, a concrete-encased ground, or a ground ring.

If these grounds are not available, the water pipe ground can be supplemented by one of the following types of grounds:

- Other local metal underground systems or structures — Local underground structures such as tanks and piping systems.
- Rod and pipe electrodes - A 5/8-in. (1.6 cm) solid rod or 3/4-in. (2 cm) conduit or pipe electrode driven to a minimum depth of 8 ft. (2.4 m).
- Plate electrodes — A minimum of 2 sq. ft. (0.185 sq. m) of metallic surface exposed to the exterior soil.

● Concrete encased ground

An electrode encased by at least 2 in. (5.1 cm) of concrete and located within and near the bottom of a concrete foundation or footing in direct contact with the earth. The electrode must be at least 20 ft. (6.1 m) of one or more steel reinforcing bars or rods, 1/2-in. (1.3 cm) in diameter, or at least 20 ft. (6.1 m) of bare solid copper, 4 AWG (26mm²) wire.

● Ground ring

A buried ground that encircles a building or structure at a depth of at least 2.5 ft (0.76 m) below the earth's surface. The ground ring must be at least 20 ft. (6.1 m) of 2 AWG (35 mm²), bare copper wire.

● Approved floor grounds

Floor grounds are those grounds on each floor of a high-rise building that are suitable for connection to the ground terminal in the riser closet and to the cabinet single-point ground terminal.

Approved floor grounds may include the following:

- Building steel
- Grounding conductor for the secondary side of the power transformer feeding the floor
- Metallic water pipes
- Power-feed metallic conduit supplying panel boards on the floor
- Grounding point specifically provided in the building for that purpose



WARNING:

If the approved ground or approved floor ground can only be accessed inside a dedicated power equipment room, then connections to this ground must be made by a licensed electrician.

Connecting the Safety Ground

Proper grounding of the G700 Media Gateway installation safeguards the system, users and service personnel by providing protection from lightning, power surges, AC mains faults, power crosses on central office trunks, and electrostatic discharge (ESD).

Local electrical installation codes must be followed when installing G700 Media Gateways.

**WARNING:**

Connection of both grounds (through the AC or DC Power Cord and the Supplementary Ground Conductor) is required for safe operation of the G700 Media Gateway.

**WARNING:**

An improper ground can cause electrical shock as well as equipment failures and service outages.

To attach the ground wires

1. Remove the ground screw on the rear of the chassis adjacent to the ground symbol:



2. Place the ring terminal of the 10 AWG (4.0 mm²) Supplementary Ground Conductor on the screw.
3. Replace the ground screw to the chassis and securely tighten the screw such that it cannot be loosened without the use of a tool.

The ground block is provided for use with more than one G700 (or other Cajun devices) in the rack. It is usually mounted by the customer electrician.

If the ground block has been purchased: Proceed with step 4; otherwise, proceed with step [7](#).

4. Cut the Supplementary Ground Conductor (which has one end attached to the grounding screw on the chassis) to the length needed to terminate it into one of the terminals of the ground block.

Do not coil the Supplementary Ground Conductor.

5. Attach one end of the remaining 10 AWG (4mm²) ground wire to one of the terminals in the ground block and the other end to an approved ground.
6. Cut this ground wire to the length needed to reach the approved ground.

Do not coil this wire.

If the ground block is not being used, simply:

7. Attach the Supplementary Ground Conductor to an approved ground.
8. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

You have now mounted the fully equipped G700 Media Gateway in the rack, cabled units together as described in the planning documents, and connected to electrical ground conductors. When all the units are mounted, cabled, and grounded, you are ready to apply power.

Connecting AC Power

For North American installations, the AC Power Cord terminates on one end with a NEMA-15P plug to connect to the AC main socket-outlet at the wall. For installations in other regions, the plug to be used must comply with the local regulations and be marked as such, be suitable for the current and voltage being used, and contain an earthing pin for connection to ground at the AC mains socket-outlet through the cord.

To prevent accidental interruption of power to the G700 Media Gateway, do not connect the G700 Media Gateway to a switch-controlled AC wall socket-outlet. In addition, Avaya Inc. highly recommends that the customer use a UPS for back-up power.

Advise your customer to verify through a licensed electrician that the ground connection at the AC outlet to be used is attached to an approved ground.

What are the G700 AC power requirements

The G700 Media Gateway uses an auto-ranging 100-240 Vac power supply, 50 to 60 Hz, 5 A maximum at 100-120 Vac and 2 A maximum at 200-240 Vac. The AC power source must be single phase, 3-conductor (Line, Neutral and Ground) with a 15 A circuit breaker for 100-120 Vac or a 10 A circuit breaker for 200-240 Vac.

Testing the AC Outlet



WARNING:

The following recommended test equipment, tests and diagrams are intended only for North American installations at 110 to 125 Volts AC. For installations in other regions, have a licensed electrician verify the ground and voltages.



WARNING:

If the AC outlet tests indicate that the power requirements are not met, your customer must contact a licensed electrician. DO NOT install the system until all requirements are met.

What are possible AC Fault Conditions

If the AC outlet tests reveal any of the following conditions, they must be corrected BEFORE the system can be installed:

- Open ground
- Hot and neutral reversed
- Open hot
- Open neutral
- Hot and ground reversed



WARNING:

Hazardous voltages are present during this test. Follow all instructions carefully when working the AC power line voltages.

To verify ground using an Ideal 61-035 Circuit Tester (or equivalent)

1. Plug the circuit tester into the outlet that you want to test.

If the circuit is properly grounded, the yellow and white lights on the tester illuminate.

2. Unplug the tester.



WARNING:

If the tester indicates any type of ground fault, your customer must contact a licensed electrician. DO NOT install the system.

To verify voltages using a Volt-Ohm Millimeter (VOM) (U.S. and countries using 110 to 125 Vac power)



WARNING:

Hazardous voltages are present during this test. Follow all instructions carefully when working with AC power line voltages.

1. Ensure that the VOM is set to read Volts AC

Note:

The following example is for North American voltages (110 to 125 Vac). Use the appropriate voltages for local power.

2. Set the VOM to the lowest scale on which you can read 130 Vac.

3. Measure the AC voltages in the following order:

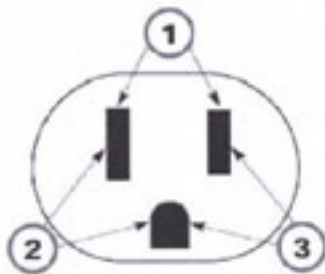


Figure notes:

1. Phase to neutral should be 110 to 125 Vac.
2. Neutral to ground should be less than 1 Vac.
3. Phase to ground should be 110 to 125 Vac.



WARNING:

If the voltage readings do not measure the values given, the AC outlet is improperly wired — DO NOT INSTALL THE SYSTEM. Advise the customer to have a licensed electrician correct the problem.

Once the ground and voltages have been verified to be correct for the installation, you are now ready to power the system.

Plugging in AC power

To connect to AC power

1. Plug the power cord into the G700
2. Plug the power cord into the outlet that was tested.

Note:

There is no On/Off power switch on the G700 Media Gateway. The AC inlet serves as the disconnect device. To disconnect power from the G700 Media Gateway, remove the power cord plug from the AC inlet.

The G700 Media Gateway powers up. The LEDs on the media modules, the S8300 Media Server, and the G700 Media Gateway flash at power-up. Each element conducts a series of self-tests.

3. The LEDs on the G700 LED panel flash, and the red ALM LED lights up until the self-tests on the G700 Media Gateway have completed.
4. The LEDs on the S8300 Media Server light as described in the following sequence:
 - a. ALM - red - lights up, then turns off. **For an S8300C only**, during the BIOS boot, the ALM LED is on (not flashing). When the BIOS boot finishes, the ALM LED starts flashing to indicate that all hardware diagnostics have passed and the system is ready to load the OS. The ALM LED continues to flash until the Avaya software is installed. The ALM LED turns off when the Avaya Linux drivers are installed.

- b. TST (S8300B) or APP (S8300C) - green – lights up, then turns off
- c. ACT - yellow – lights up, then turns off
- d. OK To REMOVE - green - lights up, then turns off
- e. LEFT LED in SERVICES port - green (10 MB link speed) lights up, then turns off
- f. LEFT LED in SERVICES port - yellow (100 MB link speed) lights up, then turns off
- g. RIGHT LED in SERVICES port - green lights up, then turns off

When you first power up the S8300, the red Major Alarm LED lights. During startup, self-tests run, after which all LEDs turn off. At this point, you can connect to the S8300. When Communication Manager starts, the green TST/APP LED turns on and stays on.

5. Verify the following LED's status:

- On the media modules: all LEDs are off.

Note:

If the initial administration of all media modules is not completed, an alarm LED will light.

- The master LED (labeled MSTR) or the system LED (labeled SYS) lights on one and only one module in the stack.
- On the G700 media gateway, the green CPU LED is illuminated, when both the P330 Stack Processor (Layer 2 Switching Processor) and the G700 Media Gateway Processor (MGP) are in a normal operational state.

The red ALM LED lights whenever an alarm exists in the G700 Media Gateway Processor. The ALM LED might signal either a hardware failure or a software or firmware condition that could be cleared by resetting the processor. It will also light because the license file for the S8300 has not yet been installed. For an S8300C only, the ALM LED flashes when the BIOS is rebooted. If it does not stop flashing, then there may be a problem with the hard drive. For an S8300C also, the ALM LED lights steadily when the S8300 has been shutdown.

Checking and Connecting DC Power

Note:

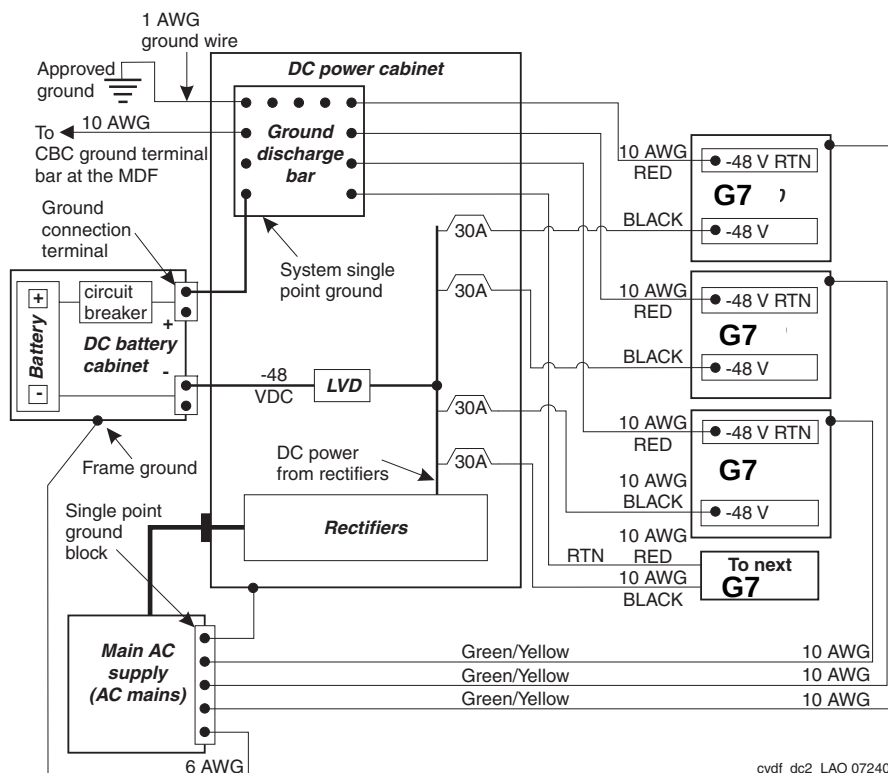
Perform this check procedure only if you are installing a G700 that is using the DC input-power option rather than AC input-power.

Before you connect the G700 media gateway DC feed cable to the DC power source, check the DC power source using a KS-20599 digital voltmeter (or equivalent).

To check DC power

1. Verify that the meter reads between -41Vdc and -56 Vdc across the -48Vdc and -48V Return distribution leads from the DC source.
2. Verify that the meter reads 0V between the -48V Return lead of the DC power source and the approved ground.
3. If either step 1 or step 2 fails the verification, **DO NOT PROCEED with step 4.**
Request that a qualified electrician resolve the problem.
4. Connect the DC feed cable for each G700 to the G700 chassis.
5. Connect the DC feed cable for each G700 to the DC power source.
 - a. Connect the red insulated 10 AWG lead to the -48Vdc Return (positive) source.
 - b. Connect the black insulated 10 AWG lead to the -48Vdc (negative) source.

Figure 16: DC Wiring Diagram



You have now completed the initial installation of the G700 Media Gateway.

Section 2: G700 installation and upgrades - wizards

This section contains procedures to install or upgrade an Avaya G700 Media Gateway controlled by an Avaya S8300, S8400, S8500, or S8700-series Media Server, using one of the available Avaya wizard tools. Information on connecting telephones and adjuncts to the G700 is presented in [Chapter 7: Telephones and adjunct systems](#).

Three tools are available for your use (for the latest versions, go to <http://support.avaya.com/avayaiw>):

- Avaya Installation Wizard
See *Job Aid: Avaya Installation Wizard*, 555-245-754.
- Gateway Installation Wizard
See *Job Aid: Avaya Gateway Installation Wizard*, 555-245-756.
- Upgrade Tool
See *Job Aid: Upgrade Tool and Worksheets*, 555-245-757.

Note:

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

This section is organized into the following chapters:

- [Chapter 3: Installing a new G700 with an S8300 using the Avaya Installation Wizard](#)
- [Chapter 4: Installing a new G700 without an S8300 using the Gateway Installation Wizard](#)
- [Chapter 5: Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool](#)
- [Chapter 6: Upgrading an existing G700 without an S8300 using the Upgrade Tool](#)

Note:

Manual procedures to perform these tasks have been retained for completeness, and may be found in [Section 3: G700 installation and upgrades - manual procedures](#).

About the Installation Roadmap and Task Lists

From your planning sheets, you can determine what type of installation or upgrade is involved with the G700 Media Gateway. Use [Table 7](#) to determine which task list is most appropriate for your upgrade or installation.

Table 7: Task lists for your upgrade or installation using the Wizards

	G700 with an S8300 (Primary or LSP)	G700 without an S8300
New Installation	Chapter 2 Chapter 3	Chapter 2 Chapter 4
Upgrade an Existing System	Chapter 5	Chapter 6

Chapter 3: Installing a new G700 with an S8300 using the Avaya Installation Wizard

This chapter covers the procedures to install a new Avaya G700 Media Gateway with an Avaya S8300 Media Server. The S8300 can be configured as either the primary controller or as a local survivable processor (LSP).

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

The G700 ships with the firmware installed on the G700 processors and media modules. However, you may need to upgrade Communication Manager, G700 firmware, and/or media module firmware if the latest available versions are not currently installed.

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

Note:

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

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

- The version of Communication Manager on the LSP must be the same as, or later than, the version running on the primary controller.
- For an LSP, you administer Communication Manager translations on the primary controller, *not* on the LSP. The primary controller then copies the translations to the LSP.



Important:

The Avaya Installation Wizard (IW) is used to configure the server ([Using the Avaya Installation Wizard \(IW\)](#) on page 133) and install G700 firmware after the Communication Manager software is installed. Other tasks have to be done manually, and are identified in the sections to follow.

Installation Overview

About software and firmware files

A new S8300 Media Server comes with a blank hard drive. The G700 components should have current releases of firmware installed. It may be necessary to install a service pack on the S8300 after installing the Communication Manager software, and/or to upgrade the G700 and media module firmware.

Communication Manager software is distributed on a CD-ROM that you take to the site. Additional files that may be needed are the most recent versions of the software service pack file and G700 firmware files. You may need to obtain these files from the Avaya Support web site.

About access to the Communication Manager software distribution CD

The R4.0 Communication Manager software and other files needed for the R4.0 installation are on the Communication Manager software distribution CD that you take to the customer site. Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate.

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

Tasks to install the S8300 and G700

Before going to the customer site

- [Obtaining a USB DVD or CD-ROM drive](#) on page 116
- [Getting information that the project manager provides](#) on page 116
- [Getting the Serial Number of the G700, if Necessary](#) on page 117
- [Checking for and FTP/SCP/SFTP Server or Compact Flash for Backing up Data](#) on page 118
- [Obtaining service pack files, if needed](#) on page 118
- [Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary](#) on page 119

- [Obtaining Ethernet interface IP address and subnet mask](#) on page 120
- [Completing the RFA process \(Obtaining license and password file\)](#) on page 120
- [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 122

Install the S8300

- [Inserting the S8300](#) on page 123
- [Setting telnet parameters](#) on page 124
- [Remastering the hard drive and installing the software](#) on page 125
- [Accessing the S8300](#) on page 128
- [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 129
- [Using the Avaya Installation Wizard \(IW\)](#) on page 133
- [Configuring an X330 Expansion Module \(if necessary\)](#) on page 172
- [Setting rapid spanning tree on the network](#) on page 173

Administer an S8300 primary controller

- [Assigning Node Names and IP Addresses for the LSPs](#) on page 175
- [Administering Network Regions](#) on page 175
- [Associating LSPs with Network Regions](#) on page 176
- [Administering IP Interfaces](#) on page 177
- [Identifying LSPs to the S8300 primary controller](#) on page 178

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

- [Assigning Node Names and IP Addresses for the C-LANs and LSPs](#) on page 180
- [Administering Network Regions](#) on page 181
- [Assigning LSPs to the Network Regions](#) on page 183
- [Administering IP Interfaces](#) on page 184
- [Identifying the Survivable Processor on the primary controller](#) on page 188

Administer the media gateway

- [Administering the Media Gateway](#) on page 189

Complete the installation of the S8300 (if the primary controller

- [Updating IA770 INTUITY AUDIX Messaging, if installed](#) on page 195
- [Backing up the system](#) on page 198
- [If using IA770, administer Communication Manager for Integrated Messaging](#) on page 200
- [Complete the Installation Process \(for an S8300 LSP\)](#) on page 200

Before Going to the Customer Site

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

Obtaining a USB DVD or CD-ROM drive

Upgrading Communication Manager on an S8300 to release 3.0 requires remastering the S8300B/C hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB DVD or CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD or CD-ROM drive at the site.

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

[Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information. However, if you are using any of the following worksheets, the setup information in the checklists are included in the worksheets:

- [Electronic pre-installation worksheet](#)
- [Name and number list](#)
- [Custom template](#)

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

Electronic pre-installation worksheet

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

Name and number list

The Name and Number List, like the EPW, is an Excel spreadsheet. The Name and Number List contains administration data for multiple users. The IW pulls this data to automatically administer users on the new system. This administration includes users' names, unicode

names (for native names in Chinese, Japanese, and other non-ASCII character languages), extensions, telephone types, classes of service, languages, locations, and voice mail capability. The Name and Number List also includes hunt group port configuration for new IA770 INTUITY AUDIX systems.



CAUTION:

For the IW to install an IA770 INTUITY AUDIX Messaging system, you *must* complete the subscriber data on the Name and Number List and then use the Name and Number List with the IW.

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

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

Custom template

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

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

Getting the Serial Number of the G700, if Necessary

For a new installation of a G700 with an S8300, you need the serial number of the G700 Media Gateway in order to complete the creation of the customer's license file on the rfa.avaya.com web site. To get this number, look for the serial number sticker on the back of the G700 chassis. If the unit is delivered directly to the customer and you will not have phone or LAN line access from the customer site to access the rfa.avaya.com web site, this task will require a preliminary trip to the customer site.

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

During the installation and upgrade procedures, you must back up the system data to an FTP, SFTP, or SCP server, or to the USB Compact Flash drive. You use a server on the customer's LAN for backups.

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



Important:

Before going to the customer site, make sure that you can use either a customer server for backups or a compact flash card.

Obtaining service pack files, if needed

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

Service packs may or may not be needed, depending on the release of Communication Manager. For both new installations and upgrades, you may need to install a service pack after the installation or upgrade. For an upgrade, you may need a service pack before the upgrade as well.

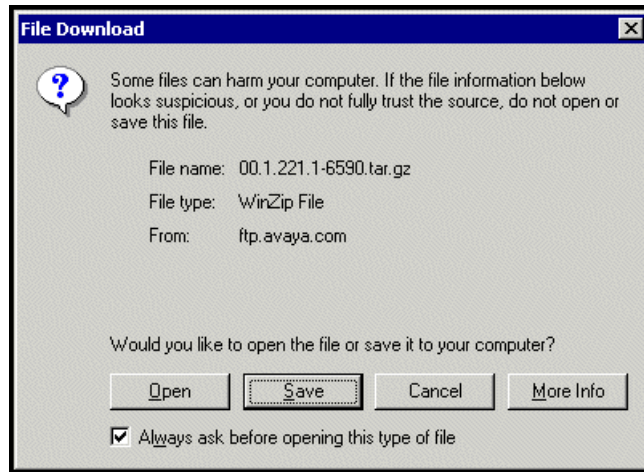
To download a pre-upgrade service pack

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

7. If you are a Business Partner, scroll to the bottom of the page and select **Download Center** to access the password protected Download Center. Otherwise, for Avaya, click on **Latest Avaya Communication Manager x.x.x Service Pack** to access the service pack download

The File Download window displays.

File download window



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

Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary

If IA700 will be installed, determine whether an service pack is needed and/or optional languages are used. If so, obtain the data files.

Obtaining an IA770 service pack file

If an IA770 service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an IA770 service pack file

1. On the Avaya Support Web site, click on **Find Documentation and Downloads by Product Name**.
2. Under the letter "I", select **IA 770 INTUITY AUDIX Messaging Application**.
3. Click on **Downloads**.

To download the IA770 patch software:

4. Click on **IA 770 INTUITY AUDIX Embedded Messaging Application Patches**.
5. Click on the service pack file name for this release.
For example, **C6072rf+b.rpm**.
6. Click on **Save** and browse to the location on your laptop where you want to save the file.

Note:

The IA770 patch documentation is co-located with the patch software.

Obtaining Optional language files

Optional languages are any language other than English (**us-eng** or **us-tdd**). If optional languages will be used with this IA770, you can also download the appropriate language files from the Download Web site.

1. Follow the steps as in [Obtaining an IA770 service pack file](#) on page 119.
2. At step [4](#), select **IA 770 INTUITY AUDIX Embedded Messaging Application Languages**.

Obtaining Ethernet interface IP address and subnet mask

If IA770 Integrated Messaging is to be installed, you must obtain an IP address and subnet mask to be used for the Ethernet interface for the H.323 integration. The subnet mask must be the same as that used for the media server (control network), and is entered on the Configure Server Web screen when you configure the S8300.

Completing the RFA process (Obtaining license and password file)

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

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

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

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

Note:

For an upgrade, you do not normally need to install a new authentication file (with a .pwd extension). However, if one is required, follow the same steps as with a license file.

Downloading license and password files

The license file of the S8300 as a Local Survivable Processor must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300, S8400, S8500, S8700, S8710, or S8720 Media Server). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

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

Note:

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

To download the license and password files to your laptop



Tip:

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

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and password files (for example, C:\licenses).
2. Access the Internet from your laptop and go to Remote Feature Activation web site, rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and password files for the customer.
4. Check that the license and password files are complete.
You might need to add the serial number of the customer's G700.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and password files to your laptop.

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

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

Note:

Business Partners call 800-295-0099. ART is available only to Avaya associates.

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

Note:

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

To run the ART

1. Access the ART web site on your laptop at <http://art.dr.avaya.com>.
2. Select **Administer S8x00 Server products for installation script**.
 - a. Log in.
 - b. Enter the customer information.
 - c. Select **Installation Script**.
 - d. Click **Start Installation script & IP Addr Admin**.

A script file is created and downloaded or emailed to you.

3. You can use the installation script to set up an IP address and other alarming parameters automatically.

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

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

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

Install the S8300

The following manual procedures cover:

- [Inserting the S8300](#)
- [Installing Communication Manager Software](#)

Inserting the S8300

To insert the S8300



CAUTION:

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

1. Connect the DVD/CD-ROM drive to the S8300 with the following steps:

Note:

You must do this *before* you completely seat the media server in the slot.

- a. Connect the USB cable into one of the USB ports on the faceplate of the S8300.
- b. Connect the other end of the USB cable to the CD-ROM or DVD/CD-RW drive.
- c. If you are using an Addonics DVD/CD-RW drive, connect the power cord to the drive and an electrical outlet.

Note:

The TEAC drive and S8300/S8400 DVD/CD-RW drive get their power from the server over the USB connection.

- d. If you are using an Addonics DVD drive, set the power source switch on the side to **EXT**, *not* **USB**.
- e. If you are using an S8300/S8400 DVD/CD-RW drive, set the on/off switch to **On**.

Be sure to set the S8300/S8400 drive to **Off** when not in use.

2. Insert the Communication Manager Software Distribution CD in the drive.



CAUTION:

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

3. For the S8300B circuit pack only, the LED module (above slot V1) must also be removed or inserted together with the S8300. Do the following:

- Disengage the LED module and remove it from the G700.
- Insert both the LED panel and S8300B circuit pack about 1/3 of the way into the guides (the guides are in slot V1 for the S8300 and above slot V1 for the LED panel).
- Push both circuit packs (together) back into the guides, gently and firmly, until the front of each circuit pack aligns with the front of the G700.

For the S8300C circuit pack only, push the S8300 module into the slot V1 guide until the front of the S8300 module aligns with the front faceplate of the G700.

4. Secure the S8300 faceplate with the thumb screws.

Tighten the thumb screws with a screw driver.

Note:

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

5. Power up the G700 by plugging in the power cord.
6. Connect the laptop to the Services port on the faceplate of the S8300.

Installing Communication Manager Software

Note:

You cannot use the SSH protocol to access the hard drive on an S8300 Media Server that has never been installed.

Setting telnet parameters

The Microsoft telnet application may be set to send a carriage return (CR) and line feed (LF) each time you press **Enter**. The installation program interprets this as two key presses. You need to correct this before you telnet to the server.

Note:

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

To set telnet parameters

1. Click **Start > Run** to open the Run dialog box.
2. Type `telnet` and press **Enter** to open a Microsoft Telnet session.
3. Type `unset crlf` and press **Enter**.

4. Type **display** and press **Enter** to confirm that Sending only CR is set.
5. Close the window by clicking on the **X** in the upper-right corner.

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

Remastering the hard drive and installing the software

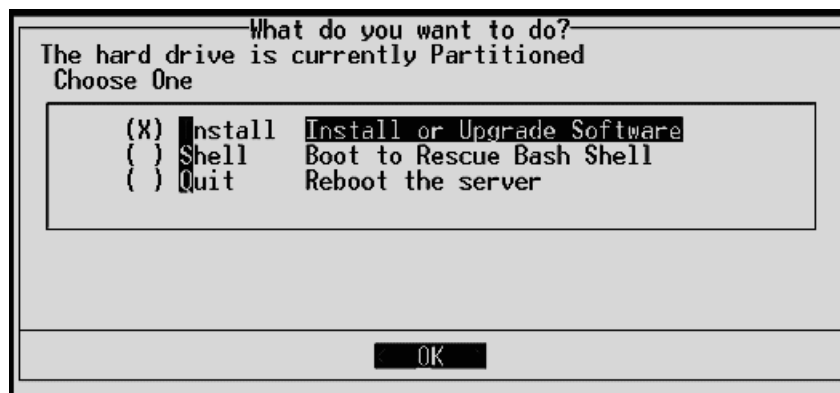
To do before you start the upgrade

1. Verify that the S8300 is inserted in slot V1.
2. Verify good AC power connections to the G700.
3. Avaya recommends using a UPS backup for media servers.
If a UPS is present, make sure the G700 is plugged into the UPS.
4. Verify that all Ethernet connections are secure, to ensure the file transfer process is not interrupted.

To begin the upgrade

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.

The first RP screen



Tip:

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

Note:

At this point, the installation script looks for the software CD on the DVD/CD drive connected to the USB port. If the DVD/CD drive was not attached to a USB port when the S8300 booted, you will not see any activity on the screen. In this case, perform the following steps:

- Press the Shut Down button on the S8300 Media Server.
- When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port and reseal the S8300 in its slot.

3. Select **Install** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen



4. Select the appropriate release version (if more than one) then select **OK** and press **Enter**.

The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen



5. Select **Yes** if you want to install IA770 concurrently with Communication Manager. Select **No** if you do not. Then press **Enter**.

Note:

If you do not install IA770 concurrently with Communication Manager at this time, and decide later to install it, you will have to upgrade Communication Manager again (even to the same release). For the upgrade, you use the Manage Software screen on the Maintenance Web interface, and select **Yes** at this screen for IA770 installation.

At this point, the following processes are initiated:

- a. The S8300 hard drive and internal Compact Flash are partitioned and reformatted.
- b. The Linux operating system is installed.
- c. Once the drive is properly configured, the program begins installing Communication Manager software and reports the progress.

Communication Manager installation progress

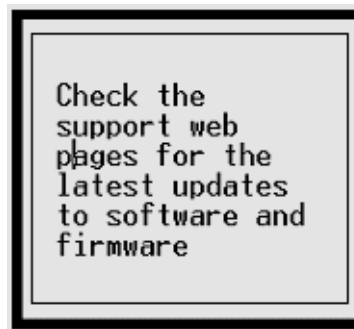
```

21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.69-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying minigetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popd-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm

```

These processes take about 30 minutes. When the media server is ready to reboot, the CD drive door opens and the following screen flashes for about 5 seconds. If selected, the IA770 software is installed along with the Communication Manager software.

Software and firmware update reminder



When the installation is complete, the system reboots automatically and the telnet connection is lost. The reboot takes 1–3 minutes without the IA770 application and 3-6 minutes if the IA770 is present.

6. Click **Start > Run** to open the **Run** dialog box on your laptop.
 7. Type `ping -t 192.11.13.6` and press **Enter**.
- Wait for the reply.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See [Laptop configuration for direct connection to the services port](#) on page 42.

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

- [Accessing the server's command line interface with SSH](#) on page 55
- [Logging in to the S8300 Web Interface from your laptop](#) on page 57

Note:

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

See [About connection and login methods](#) on page 41 for details on how physically to connect and log into the G700.

Creating a super-user login, if necessary, for R4.0 or higher

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages. Use the following steps only if you are starting from Release 4.0 software or later:

Note:

A craft level login can create a super-user login in Release 4.0 or later.

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

To create a login:

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

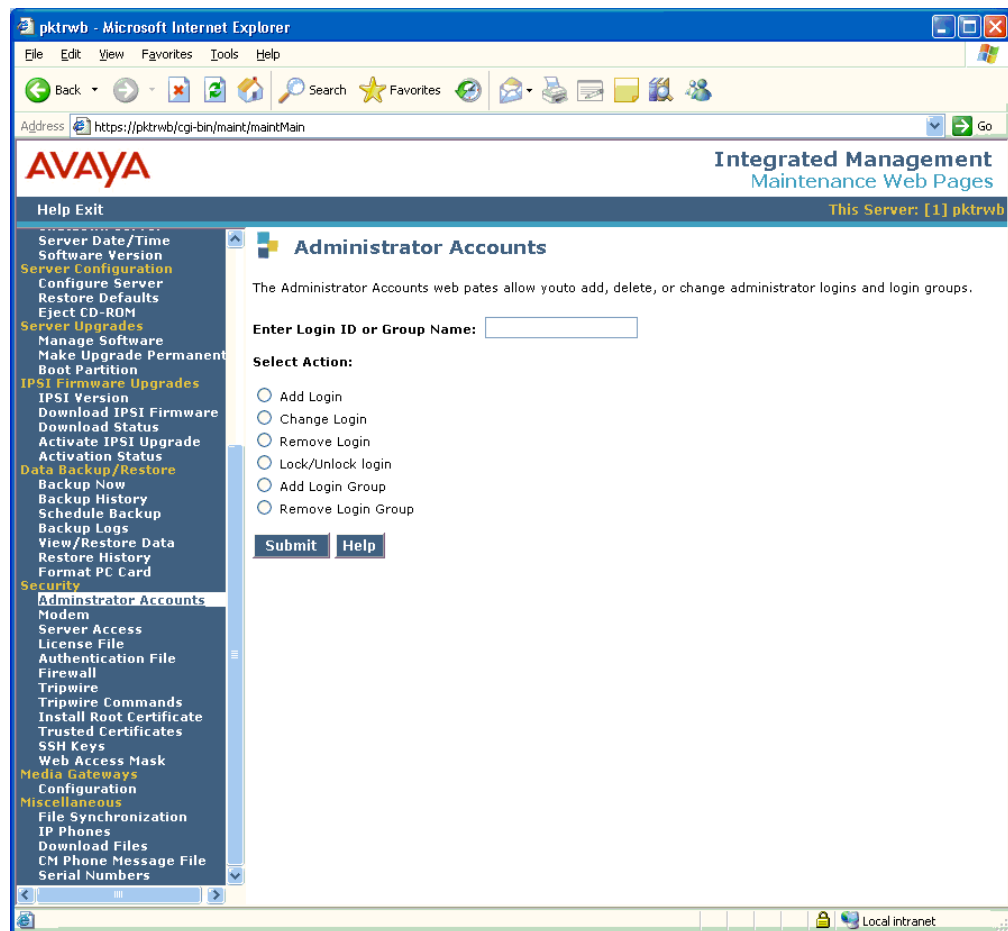
Note:

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

Installing a new G700 with an S8300 using the Avaya Installation Wizard

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



3. Type the login name in the **Enter Login ID or Group Name** field.

4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The left sidebar contains a navigation menu with categories like 'Server Upgrades', 'IPSI Firmware Upgrades', 'Data Backup/Restore', and 'Security'. The main content area is titled 'Administrator Logins -- Add Login' and contains the following form fields:

- Login ID:** Pre-filled with 'randy'.
- login group:** Text box containing 'susers'.
- additional groups:** Text box containing 'prof18'.
- allow Linux shell access:** Radio button (unchecked).
- lock this account:** Radio button (unchecked).
- date (YYYY-MM-DD) on which account is disabled (blank to ignore):** Empty text box.
- select type of authentication:** Radio buttons for 'password' (selected) and 'ASG'.
- enter key or password:** Text box.
- re-enter key or password:** Text box.
- force password/key change on first login:** Radio buttons for 'yes' and 'no' (selected).
- maximum Number of days a password may be used (PASS_MAX_DAYS):** Text box containing '90'.
- minimum number of days allowed between password changes (PASS_MIN_DAYS):** Text box containing '90'.
- minimum acceptable password length (PASS_MIN_LEN):** Text box containing '8'.
- number of days warning given before a password expires (PASS_WARN_AGE):** Text box.
- days after password expires to lock account (0=immediate):** Text box.

At the bottom of the form are 'Add' and 'Help' buttons. The status bar at the bottom shows 'Done' and 'Internet' connectivity.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

10. Complete the following fields:

- enter a challenge key or password
- re-enter challenge key or password
- force password/key change on first login

Note:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

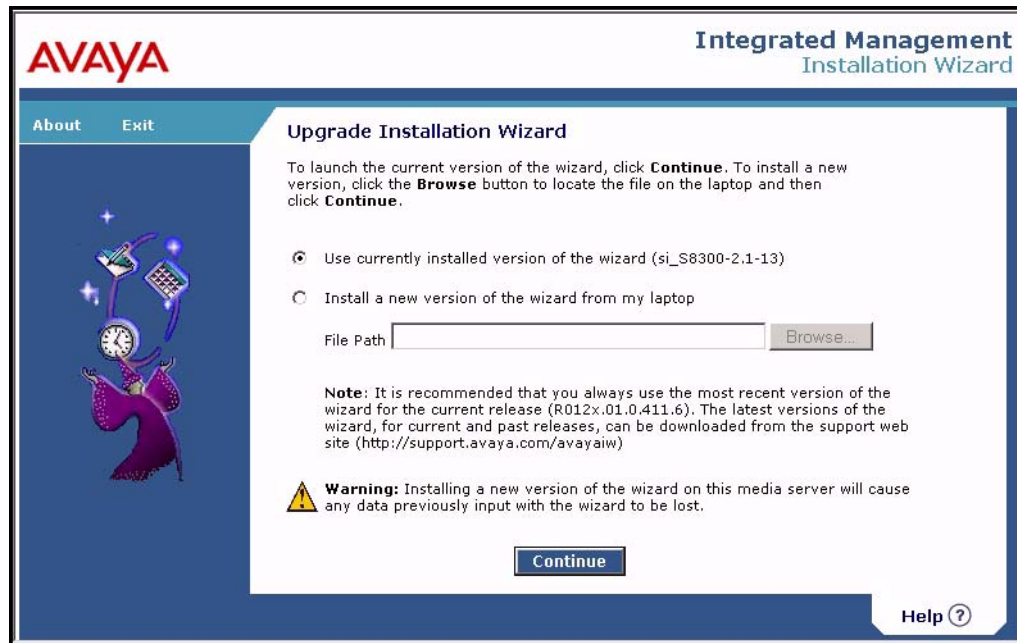
13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

- a. Log in with `telnet` or `ssh`.
- b. At the Linux command line, type `filesync -a <IP_address_of_LSP>` , where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

Using the Avaya Installation Wizard (IW)

1. Log in to the S8300 Maintenance Web page.
2. From the Maintenance Web Interface, launch the Avaya Installation Wizard. The **Upgrade Installation Wizard** screen appears.

Upgrade Installation Wizard screen



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

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

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

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

Electronic Preinstallation Worksheet screen

The screenshot shows the 'Electronic Preinstallation Worksheet' screen of the Avaya Integrated Management Installation Wizard. The left sidebar lists steps from 1 to 8, with '1 General' expanded to show sub-steps: 'Auto Discovery', 'EPW' (selected), 'Usage Options', 'Checklist', and 'Nvram Init'. The main content area explains that the wizard allows importing data from an EPW file. It includes a checkbox for 'Import EPW' and a 'Browse...' button for the 'File Path'. A warning icon and text state: 'WARNING: Do NOT import an EPW file if you are using this wizard to upgrade an existing media server with new Avaya Communication Manager software and/or media gateway firmware.' A note mentions that the EPW is an Excel document available on the Avaya support site. At the bottom, there are 'BACK' and 'CONTINUE' buttons, and a 'Help' link.

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

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

Usage Options screen

The screenshot shows the 'Usage Options' screen of the Avaya Integrated Management Installation Wizard. The left sidebar shows steps 1 to 5, with '1 General' expanded to show sub-steps: 'Auto Discovery', 'EPW', 'Usage Options' (selected), 'Checklist', and 'Nvram Init'. The main content area explains that the wizard can be used for media server installation or upgrading. It includes sections for 'IP Defaults' with a checked checkbox for 'Display current IP address information as read from the media server and gateway.', and 'Wizard Usage' with three radio button options: 'Install this media server as a Main Server' (selected), 'Install this media server as an LSP', and 'Upgrade a previously installed media server with new software and/or media gateway firmware'. At the bottom, there are 'BACK' and 'CONTINUE' buttons, and a 'Help' link.

7. Select either **Install this media server as a Main server** or **Install this media server as an LSP**. Leave the **IP Defaults** checkbox unchecked.
8. Click **Continue**, after which you will be asked to confirm your choice of Wizard Usage before continuing.

After reviewing a checklist of required and optional items for continuing the installation, you then have the option to run the `nvrnm initialize` command, which restores all factory default settings on all available media gateways, as well as the P330 Stack Processor. For a new installation, this is unnecessary.

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

The **Date/Time** screen appears.

Date/Time screen

AVAYA Integrated Management Installation Wizard

About Exit

Steps

- 1 General
- 2 Media Server
 - Date/Time**
 - Product ID
 - Software Upgrade
 - Software Update
 - Unicode Install
 - Media Server IP
 - Stack Processor
 - Optional Services
 - Translations
 - Security Files
- 3 Media Gateways
- 4 Telephony
- 5 Trunking
- 6 Endpoints
- 7 Alarm

Date/Time

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

☒ Use current date/time settings

Date **2/22/2005** (mm/dd/yyyy)

Time **10:00:05** (hh:mm:ss) Use 24-hour format

Time Zone **US (MST)**

☐ Reset date/time to the following:

Date (mm/dd/yyyy)

Time (hh:mm) Use 24-hour format

Time Zone

BACK CONTINUE Help ?

10. Choose the current date and time information that the IW detects on the S8300. If necessary, you can reset the date, time, and time zone.

CAUTION:

If you are installing an LSP, you must set the time of the LSP to the same time zone as the primary controller even if the LSP is physically located in a different time zone.

11. Click **Continue**.

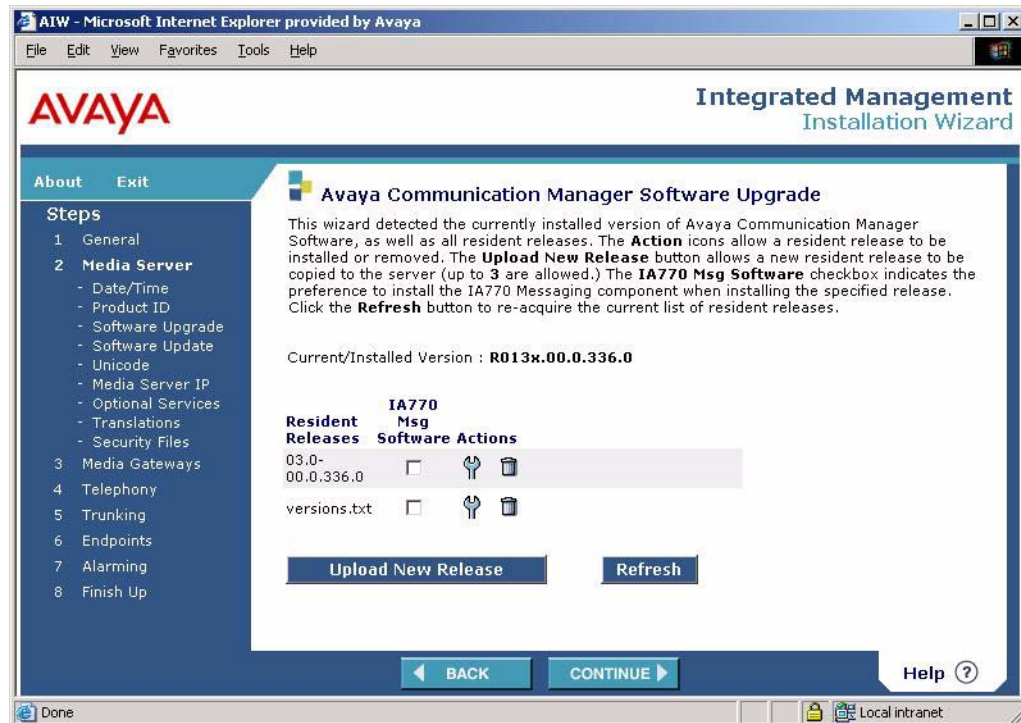
The IW displays the Product ID screen, which Avaya installers use. The screen is not used by business partners.

Installing a new G700 with an S8300 using the Avaya Installation Wizard

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

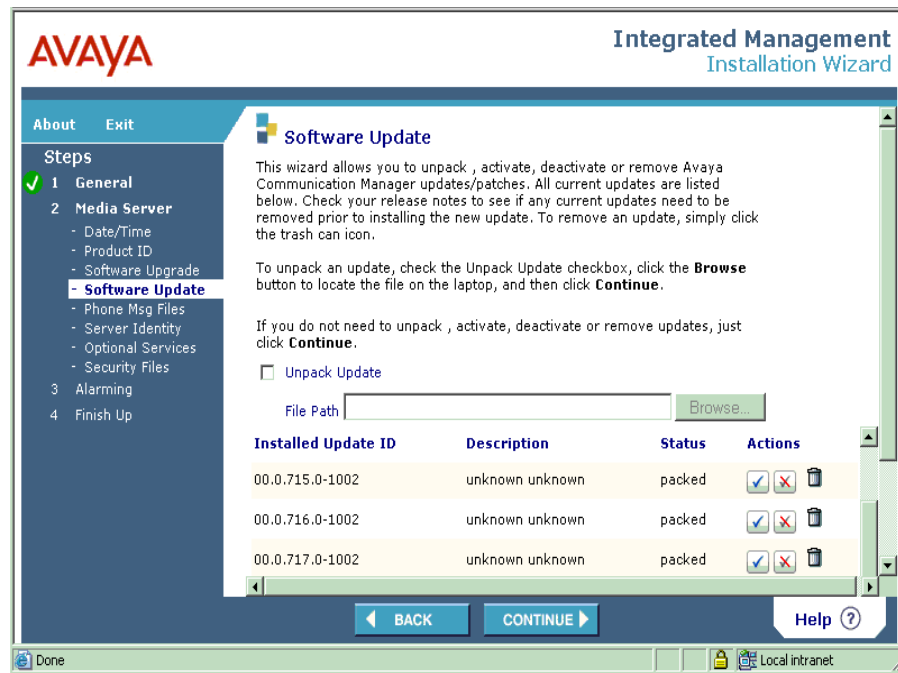
The **Avaya Communication Manager Software Upgrade** screen displays the version of Communication Manager you just installed appears.

Avaya Communication Manager Software Upgrade screen



- Click **Continue**.

The Software Update screen appears.



13. Do one or both of the following:

- If there is an update or security file you need to download, click the **Browse** button to locate the file. If the file you are downloading needs to be unpacked, click the **Unpack** box.
- If there are earlier versions of files that you are updating, select those versions and click **Deactivate**.

The screen shows the status of the deactivation.

- If a file you want to activate shows **packed** in the **Status** column, select that file and click **Unpack**.

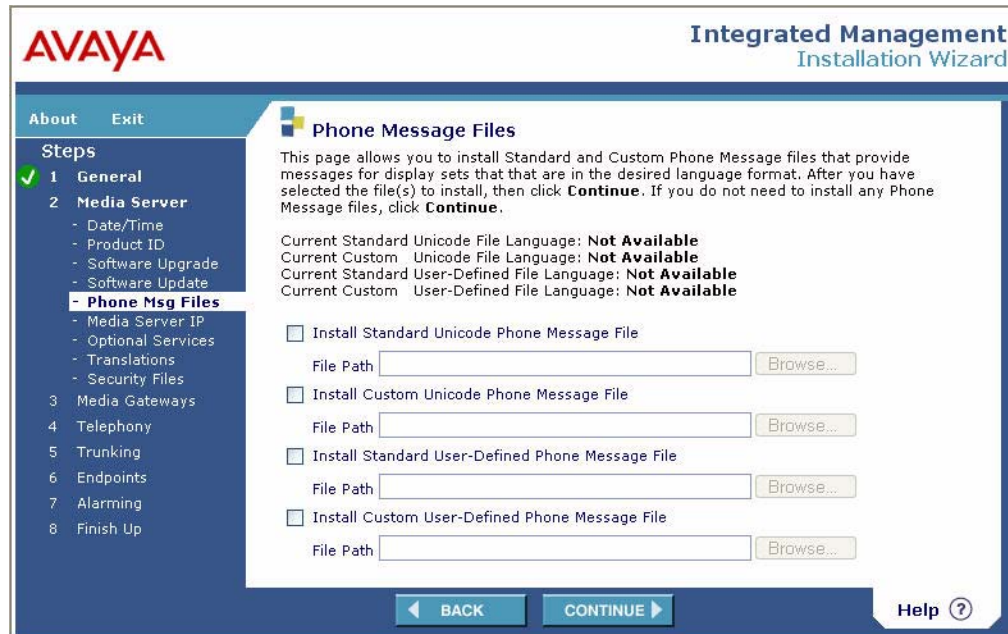
The screen shows the status of the unpacking.

14. Check the **Description** for the file you want to activate. Tell the customer that the system will reboot if the file type is **cold**. The customer may want to wait to install this security update.

15. Select the file you want to activate and click **Activate**.

16. Click **Continue**.

The Install Unicode Phone Message Files screen appears. This screen allows you to install files that provide unicode messages for display sets that are in the desired unicode language format.



17. Click **Continue**.

The Media Server - IP Addresses screen appears. If your S8300 media server is already configured, the Avaya IW should detect and display its address information in this screen. If not, you must enter the required information.

The screenshot shows the 'Media Server - IP Addresses' configuration screen within the Avaya Integrated Management Installation Wizard. The left sidebar lists the installation steps, with '1 General' and '2 Media Server' expanded. Under 'Media Server', the 'Media Server IP' sub-step is selected. The main area contains fields for Host Name (aiw-g250t1-icc), IP Address (135.9.77.131), Subnet Mask (255.255.255.0), and Default Gateway (135.9.77.254). There is also a field for IA770 IP Integration IP Address, which is currently blank. A warning message states: 'WARNING: The IA770 IP Integration IP Address field should **only** be populated if the switch is to be set up for IA770 With IP Integration. For IA770 With Hardware Integration, the field **must** be blank!'. At the bottom, there are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

18. Click **Continue**.

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

Installing a new G700 with an S8300 using the Avaya Installation Wizard

19. Click **Continue**.

The P330 Stack Processor - IP Addresses screen appears.

The screenshot shows the 'P330 Stack Processor - IP Addresses' screen in the Avaya Integrated Management Installation Wizard. The left sidebar lists the steps: 1 General (checked), 2 Media Server, 3 Stack Processor, 4 Media Gateways, 5 Telephony, 6 Trunking, 7 Endpoints, 8 Alarming, and 9 Finish Up. The main area contains the following information:

P330 Stack Processor
Configure the P330 stack processor to access the LAN. Type the required information and then click **Continue**.

IP Address: 135.9.80.89
Subnet Mask: 255.255.255.0
VLAN Number: 1

Add IPRoutes ...

IP Routes	Destination IP Address	Default Gateway IP Address
1	0.0.0.0	135.9.80.254

Buttons: BACK, CONTINUE, Help ?

20. Add the data as appropriate.

21. The Optional Services screen appears. Select the services you want.

The screenshot shows the 'Optional Services' screen in the Avaya Integrated Management Installation Wizard. The left sidebar lists the steps: 1 General (checked), 2 Media Server, 3 Stack Processor, 4 Media Gateways, 5 Telephony, 6 Trunking, 7 Endpoints, 8 Alarming, and 9 Finish Up. The main area contains the following information:

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

☐ Uninterruptable Power Supply (UPS)
☐ Domain Name Service (DNS)
☐ Network Time Protocol (NTP)
☐ Remote Access/INADS Support

Buttons: BACK, CONTINUE, Help ?

22. Click **Continue**.

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

The screenshot shows the Avaya Integrated Management Installation Wizard (IW) window. The title bar reads "AVAYA Integrated Management Installation Wizard". The window has a blue header and a sidebar on the left. The sidebar contains a "Steps" list with the following items: 1 General (checked), 2 Media Server (with sub-items: Date/Time, Product ID, Software Upgrade, Software Update, Unicode, Media Server IP, Optional Services), - UPS (with sub-items: Translations, Security Files), 3 Media Gateways, 4 Alarming, and 5 Finish Up. The main content area is titled "Uninterruptible Power Supply (UPS)" and contains the instruction: "Identify the UPS system on the network for this solution. Type the required information and then click **Continue**." Below this instruction are three input fields: "UPS IP Address", "SNMP (Read) String", and "SNMP (Write) String". At the bottom of the main area are two buttons: "BACK" and "CONTINUE". A "Help ?" link is located in the bottom right corner of the main area. The Windows taskbar at the bottom shows the "Done" button and the "Local intranet" icon.

AVAYA Integrated Management Installation Wizard

About Exit

Steps

- ✓ 1 General
- 2 Media Server
 - Date/Time
 - Product ID
 - Software Upgrade
 - Software Update
 - Unicode
 - Media Server IP
 - Optional Services
- UPS
 - Translations
 - Security Files
- 3 Media Gateways
- 4 Alarming
- 5 Finish Up

Uninterruptible Power Supply (UPS)

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

UPS

UPS IP Address

SNMP (Read) String

SNMP (Write) String

BACK CONTINUE

Help ?

Done Local intranet

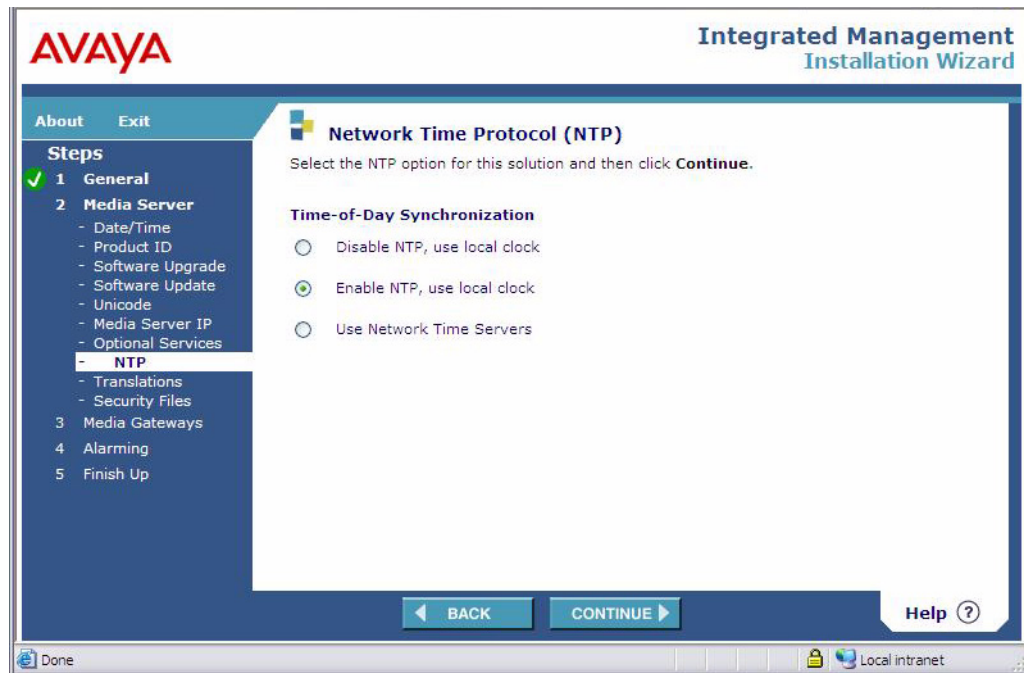
23. Click **Continue**.

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

The screenshot shows the 'Domain Name Server (DNS)' configuration window of the Avaya Integrated Management Installation Wizard. The window has a blue header with the Avaya logo and the title 'Integrated Management Installation Wizard'. On the left, a 'Steps' sidebar lists the installation process: 1. General (selected with a green checkmark), 2. Media Server (with sub-items: Date/Time, Product ID, Software Upgrade, Software Update, Unicode, Media Server IP, and Optional Services), 3. Media Gateways, 4. Alarming, and 5. Finish Up. The main content area is titled 'Domain Name Server (DNS)' and includes the instruction: 'Identify the DNS servers on the network for this solution. Type the required information and then click **Continue**.' Below this, there are three sections: 'DNS Servers' with three IP Address input fields (the first contains '135.9.1.2', the second '135.9.1.38' and is marked '(Optional)', and the third is empty and marked '(Optional)'); 'DNS Domain' with a 'Domain Name' input field containing 'dr.avaya.com'; and 'Domain Name Search Order' with four input fields (the first contains 'dr.avaya.com', the second 'avaya.com', and the last two are empty). At the bottom of the main area are 'BACK' and 'CONTINUE' buttons. A 'Help ?' link is in the bottom right corner. The Windows taskbar at the bottom shows 'Done' on the left and 'Local intranet' on the right.

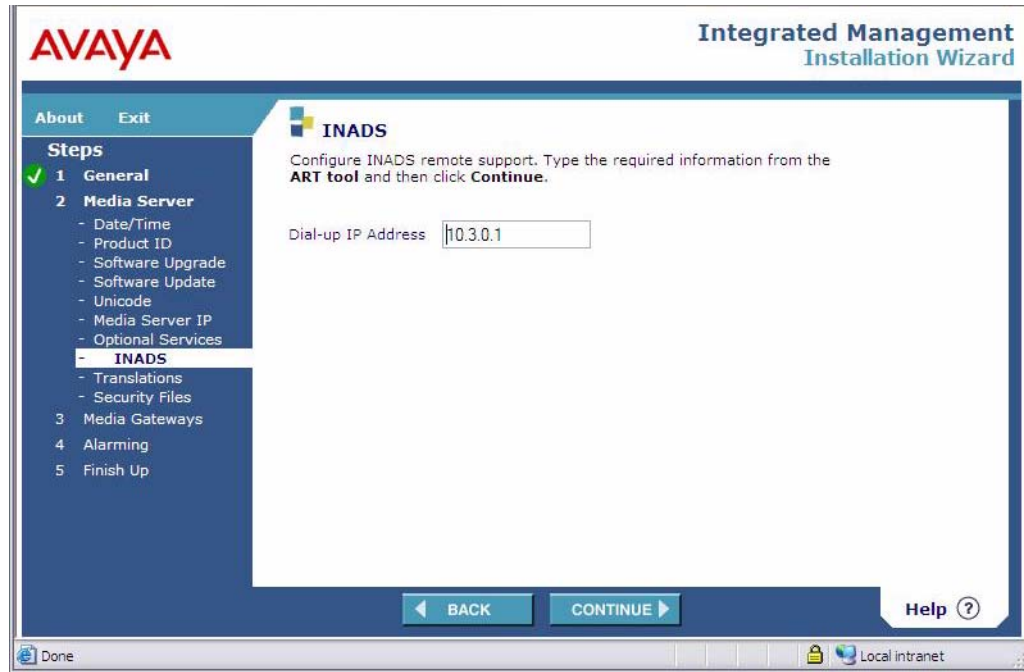
24. Click **Continue**.

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



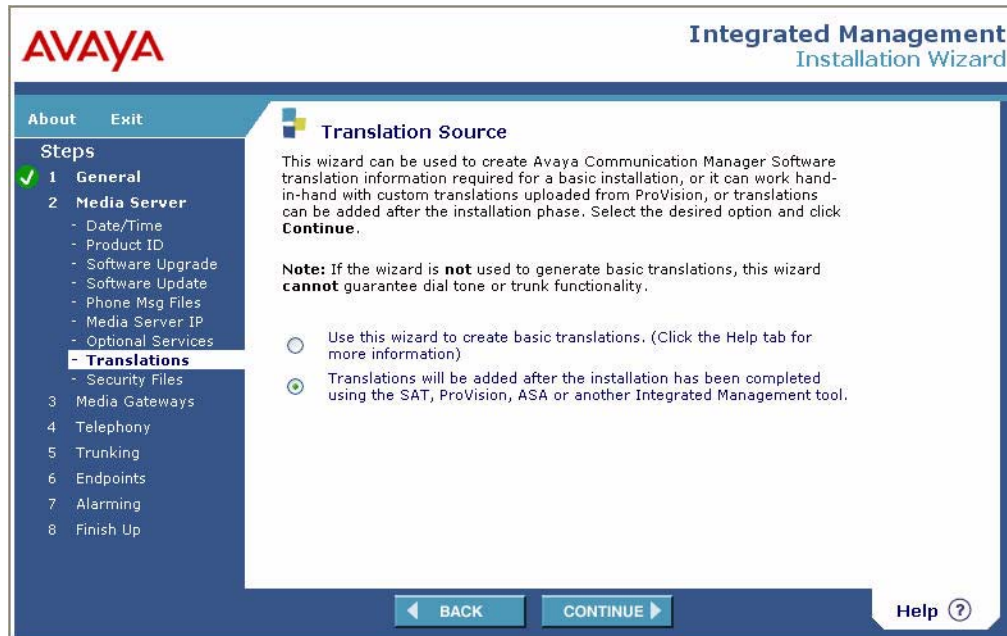
25. Click **Continue**.

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



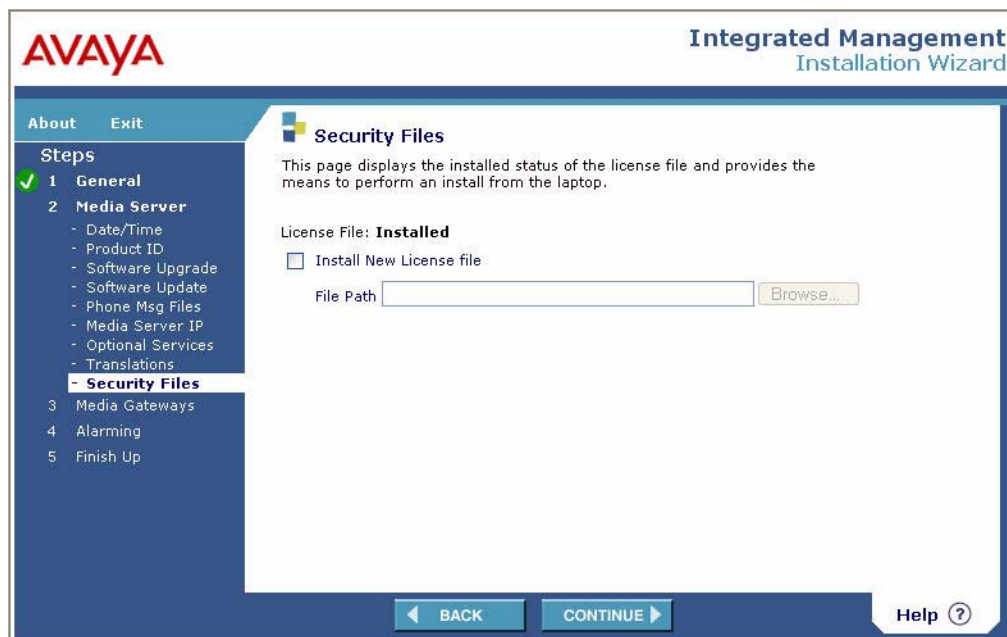
26. Click **Continue**.

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



27. Click **Continue**.

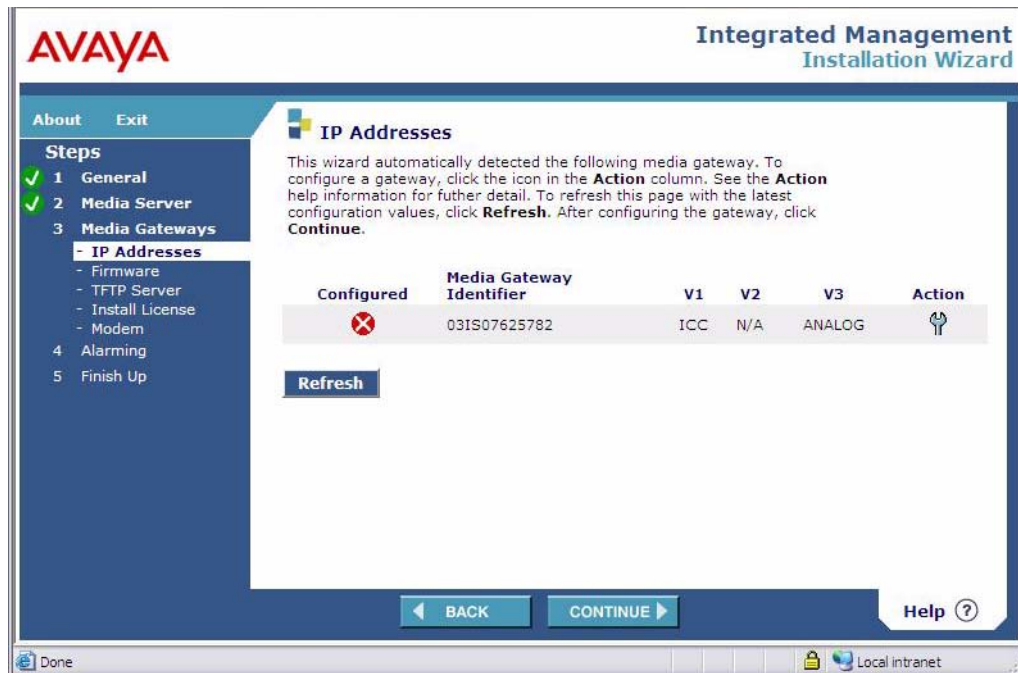
The Security Files screen appears. This screen displays the status of your license file, and allows you to install this file from a laptop.



Installing a new G700 with an S8300 using the Avaya Installation Wizard

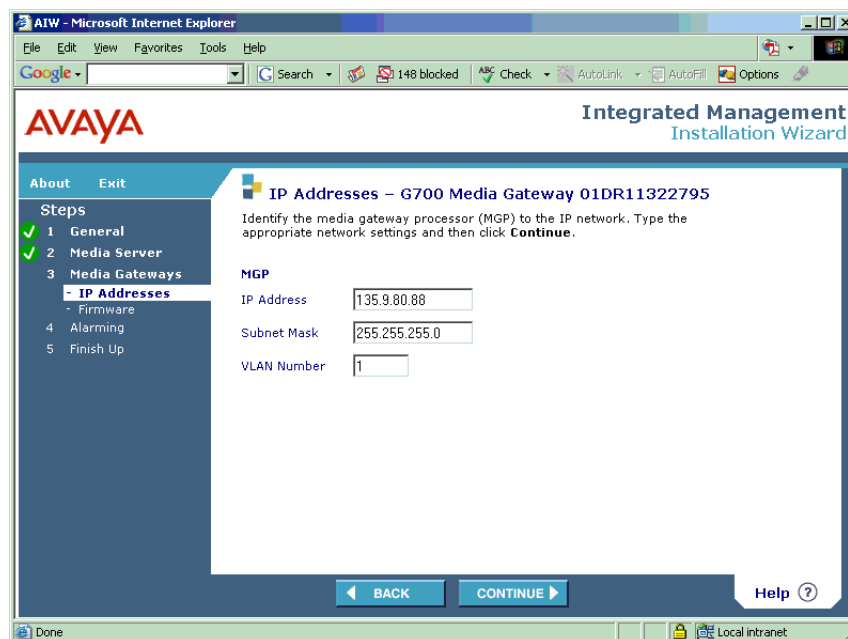
28. Click **Continue**.

The IP Addresses screen appears. This screen displays the G700's ID, as well as the type of media module residing in each slot of the G700's chassis.



29. To continue, click the icon corresponding to the G700 in the **Action** column.

The IP Address - G700 Media Gateway screen appears.



30. Enter the following information:

- **IP Address** — the IP address assigned to the Media Gateway Processor
- **Subnet Mask** — the subnet mask assigned to the Media Gateway Processor
- **VLAN Number** — the VLAN assigned to the Media Gateway Processor, normally the same VLAN assigned to the primary controller

31. Click **Continue**.

The Static Route screen appears.

AVAYA Integrated Management Installation Wizard

About Exit

Steps

- 1 General
- 2 Media Server
- 3 Media Gateways
 - IP Addresses
 - Firmware
- 4 Alarming
- 5 Finish Up

IP Addresses – G700 Media Gateway 02DR01130354

Click the **Add IPRoute Button** to configure additional IP routes. Type the appropriate network settings and then click **Continue**.

Add IPRoutes ...

IP Routes	Destination IP Address	Destination Subnet Mask	Default Gateway IP Address
1	0.0.0.0	0.0.0.0	135.9.78.254
2	135.9.78.0	255.255.255.0	135.9.78.55

BACK CONTINUE Help ?

32. Complete the fields as follows for each IP Route number:

- **Destination IP Address** — the default 0.0.0.0 or the IP address of the destination IP route
- **Destination Subnet Mask** — the default 0.0.0.0 or the subnet mask of the destination IP route
- **Gateway IP Address** — the IP address of the default network gateway for the route



CAUTION:

The default gateway IP address is required for Communication Manager 4.0.

33. Click **Continue**.

The Media Gateway Controller Information screen appears. Configure the list of Media Gateway Controllers (MGCs) that will provide call processing services for the G700. You must specify a primary MGC in the first IP address box. You can specify up to three backup MGCs in the optional IP address boxes, in priority order. The G700 searches for the primary MGC first. If it cannot connect to the primary MGC, it searches for a backup MGC. An MGC may be the Avaya S8300 Media Server installed in the G700 or an external S8500 Media Server or Avaya S8700 Media Server, or an Avaya S8300 Media Server installed in an

Installing a new G700 with an S8300 using the Avaya Installation Wizard

external media gateway. Specify your primary MGC in accordance with the usage option you chose. If you do not configure the S8300 installed in the G700 as the primary MGC, configure the S8300 as a backup MGC.

Note:

To register an S8500 or S8700-series media server as the MGC, use the IP address of the media server's Control-LAN card (CLAN) rather than the IP address of the media server itself.

The screenshot shows the Avaya Integrated Management Installation Wizard. The left sidebar contains a 'Steps' list with five items: 1 General, 2 Media Server, 3 Media Gateways, 4 Alarming, and 5 Finish Up. The 'Media Gateways' step is expanded, showing sub-steps: IP Addresses, Firmware, Install License, Install Auth File, TFTP Server, and Modem. The main window is titled 'Media Gateway Controller Information' and contains the following text: 'Configure the media gateway controller list with the media servers that will provide call processing service for the media gateway. Additionally, configure the associated transition points used by the media gateway when searching for an alternate call processing controller in the case that the current call processing controller cannot be reached. Enter the required information and then click **Continue**.'

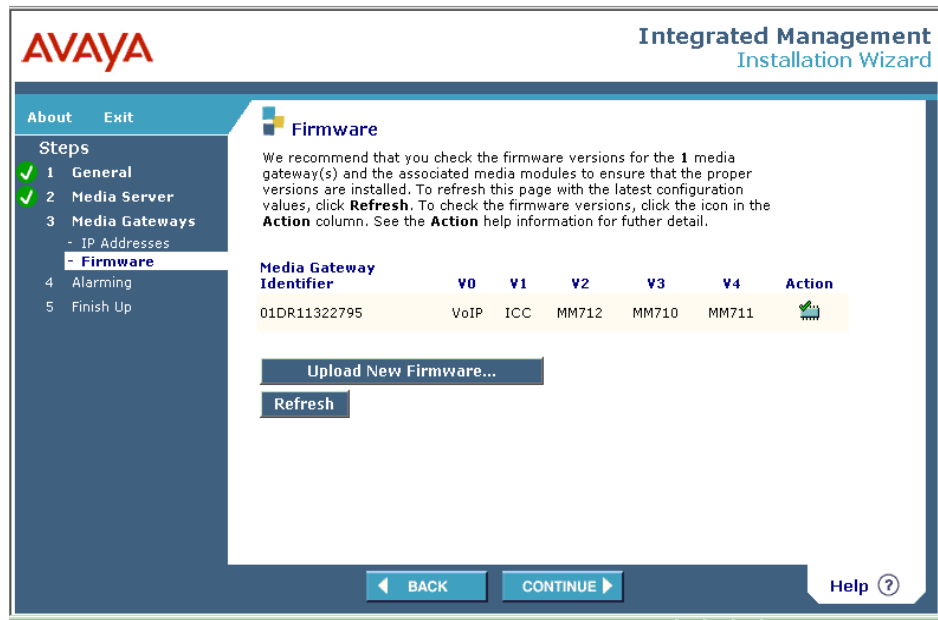
Controller	Ping Result	IP Address
1		135.9.77.131
2		(Optional)
3		(Optional)
4		(Optional)

Below the table is a 'Ping Test' button. Underneath is the 'Transition Point Information' section with three fields: 'Primary Search Time' (15 minutes), 'Total Search Time' (30 minutes), and 'Transition Point' (1).

At the bottom of the window are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

34. To upgrade the G700 firmware, click **Continue** on the Media Gateway Controller Information screen.

The Firmware screen appears.

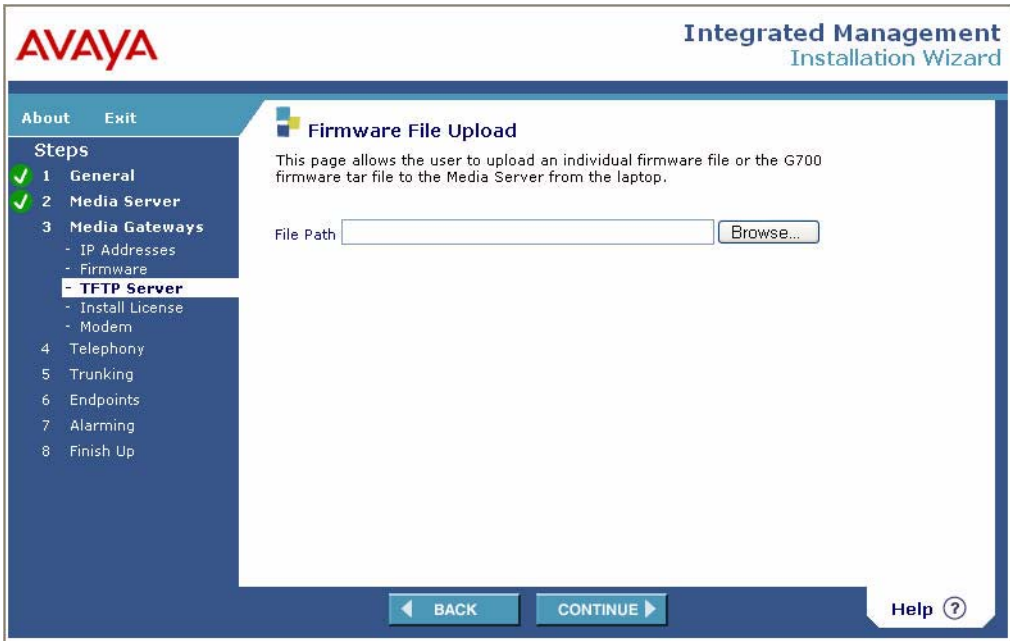


35. To upload a new firmware version from a laptop, click **Upload New Firmware**.

The Firmware File Upload screen appears. This screen allows you to upload a new firmware file from a laptop.

Installing a new G700 with an S8300 using the Avaya Installation Wizard

36. Enter the file path of the file you want to upload, or use the **Browse** button to locate the file.

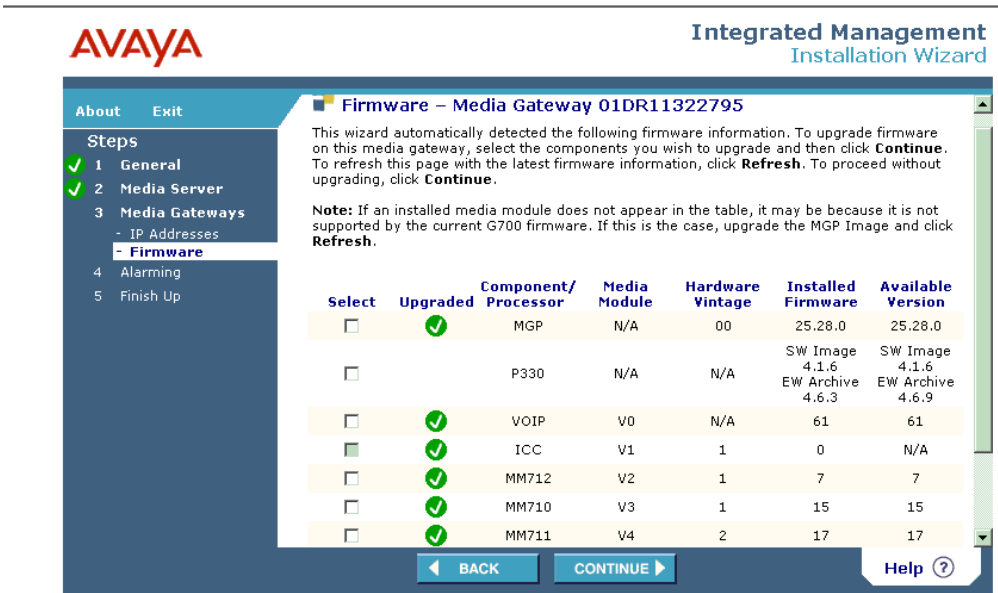


37. Click **Continue** to upload the file.

The Firmware screen appears.

38. To upgrade firmware, select the action icon.

This screen displays the currently installed firmware versions on the G700 and its media modules, as well as the most recent available versions.



39. Select the modules you want to upgrade and click **Continue**.
40. To proceed without upgrading any firmware, clear all the boxes in the **Select** column and click **Continue**.

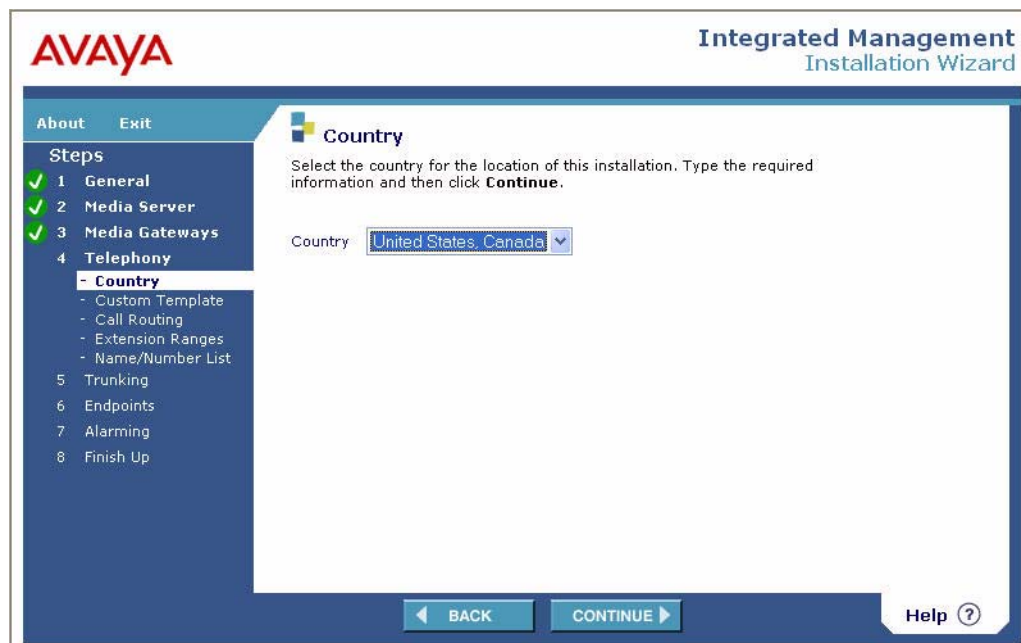
If you are adding translations using the wizard, the Country screen appears. Go to [Telephony configuration](#) on page 151.

If you are not adding translations using the wizard, the Modem Status screen appears. Go to [Alarm configuration](#) on page 164.

Telephony configuration

To configure translations, do the following:

1. On the Country screen, select the country in which the installation is taking place.



Installing a new G700 with an S8300 using the Avaya Installation Wizard

2. Click **Continue**.

The Import Custom Template screen appears. This screen allows you to configure telephony translation defaults for the Avaya IW.

The screenshot shows the 'Import Custom Template' screen of the Avaya Integrated Management Installation Wizard. The left sidebar contains a 'Steps' list with 8 items: 1 General, 2 Media Server, 3 Media Gateways, 4 Telephony, 5 Trunking, 6 Endpoints, 7 Alarming, and 8 Finish Up. Under '4 Telephony', there are sub-items: Country, Custom Template (highlighted), Call Routing, Extension Ranges, and Name/Number List. The main content area is titled 'Import Custom Template' and contains a paragraph explaining the options for configuring defaults. Below the text are three radio buttons: 'Overwrite current setting' (unchecked), 'Restore default settings' (selected), and 'Import Custom Template' (unchecked). There is a 'File Path' text box and a 'Browse...' button. A 'NOTE' at the bottom states that the Custom Template is available on the Avaya support website. At the bottom of the screen are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

AVAYA Integrated Management Installation Wizard

About Exit

Steps

- 1 General
- 2 Media Server
- 3 Media Gateways
- 4 Telephony
 - Country
 - Custom Template**
 - Call Routing
 - Extension Ranges
 - Name/Number List
- 5 Trunking
- 6 Endpoints
- 7 Alarming
- 8 Finish Up

Import Custom Template

This page gives you two options for configuring defaults used by the wizard for telephony translations. To configure the wizard defined defaults with defaults, simply click **Continue**. To import your own Custom Template that defines telephony defaults, first check the checkbox below. Then select the Import radio button, click the **Browse** button to locate the Custom Template file on your laptop, and then click **Continue**. If the system has already been configured with a Custom Template and you wish to restore the wizard defined defaults, select the Restore option and click **Continue**.

☐ Overwrite current setting

☒ Restore default settings

☐ Import Custom Template

File Path

NOTE: The Custom Template is available on the Avaya Installation Wizard's support web site (<http://support.avaya.com/avaiaw>).

[Help ?](#)

3. Click **Continue**.

The Call Routing screen appears. Enter the required call routing information.

The screenshot shows the 'Call Routing' screen of the Avaya Integrated Management Installation Wizard. The left sidebar is identical to the previous screen, with '4 Telephony' > 'Call Routing' highlighted. The main content area is titled 'Call Routing' and contains a paragraph asking the user to specify call routing information. Below the text are several input fields: '10-digit Dialing' (checked), 'Primary NPA' (303), 'Other Local NPA(s)' (three empty boxes followed by '(Optional)'), 'Attendant Access Number' (empty box followed by '(0-9) (Optional)'), and 'Voice Mail Extension' (empty box followed by '(Optional)'). At the bottom of the screen are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

AVAYA Integrated Management Installation Wizard

About Exit

Steps

- 1 General
- 2 Media Server
- 3 Media Gateways
- 4 Telephony
 - Country
 - Custom Template
 - Call Routing**
 - Extension Ranges
 - Name/Number List
- 5 Trunking
- 6 Endpoints
- 7 Alarming
- 8 Finish Up

Call Routing

Specify call routing information. Type the required information and then click **Continue**.

10-digit Dialing ☒

Primary NPA

Other Local NPA(s) (Optional)

Attendant Access Number (0-9) (Optional)

Voice Mail Extension (Optional)

[Help ?](#)

4. Click **Continue**.

The Extension Ranges screen appears.

The screenshot shows the 'Extension Ranges' screen of the Avaya Integrated Management Installation Wizard. The interface includes a sidebar with a 'Steps' list, a main content area with instructions and a table, and a bottom navigation bar.

AVAYA Integrated Management Installation Wizard

About Exit

Steps

- ✓ 1 General
- ✓ 2 Media Server
- ✓ 3 Media Gateways
- 4 **Telephony**
 - Country
 - Custom Template
 - Call Routing
 - **Extension Ranges**
 - Name/Number List
- 5 Trunking
- 6 Endpoints
- 7 Alarming
- 8 Finish Up

Extension Ranges

This page allows you to specify the extension ranges you will support with this S8300 media server. Click the **Add Extension Range** button and then enter the starting and ending extensions for the range. Then check the Private Networking checkbox if the extension range will be used to route calls over an IP trunk. When you have finished entering all the extension ranges you need, click **Continue**.

Add Extension Range...

Extension Range	Starting Extension	Ending Extension	Private Networking?	Actions
1	1000	2000	☐	

◀ BACK CONTINUE ▶ Help ?

5. To add a range, click **Add Extension Range** and enter the starting and ending extensions for the range. If you want this range to be used to route calls over an IP trunk, select **Private Networking**. To add additional extension ranges, repeat these steps. When you are finished, click **Continue**.

The Import Name/Number List screen appears. This screen allows you to import an Excel file that contains user names, extension numbers, and other information.

The screenshot shows the 'Import Name/Number List' screen of the Avaya Integrated Management Installation Wizard. The Avaya logo is in the top left, and the title 'Integrated Management Installation Wizard' is in the top right. A left sidebar contains a 'Steps' list with items 1 through 8: 1 General, 2 Media Server, 3 Media Gateways, 4 Telephony (with sub-items Country, Custom Template, Call Routing, and Extension Ranges), 5 Name/Number List (highlighted), 6 Trunking, 7 Endpoints, 8 Alarming, and 9 Finish Up. The main content area is titled 'Import Name/Number List' and contains instructions: 'Import an Excel file that contains the user names, extension numbers, model numbers of terminal end points, user locations, whether or not users have voice mail, COS, and display languages. To install the file, type the path name or click **Browse**. After installing the file, click **Continue**.' Below this is a checkbox labeled 'Import the following name and number list'. Under the checkbox is a 'File Path' text box and a 'Browse...' button. A 'NOTE' states: 'The Name/Number List is available on the Avaya Installation Wizard's support web site (<http://support.avaya.com/avayaiw>).'. At the bottom are 'BACK' and 'CONTINUE' buttons, and a 'Help ?' link in the bottom right corner.

To import this file:

- a. Select **Import the following name and number list**.
- b. Enter the file path of the file you want to import, or use the **Browse** button to locate the file.
- c. Click **Continue**.

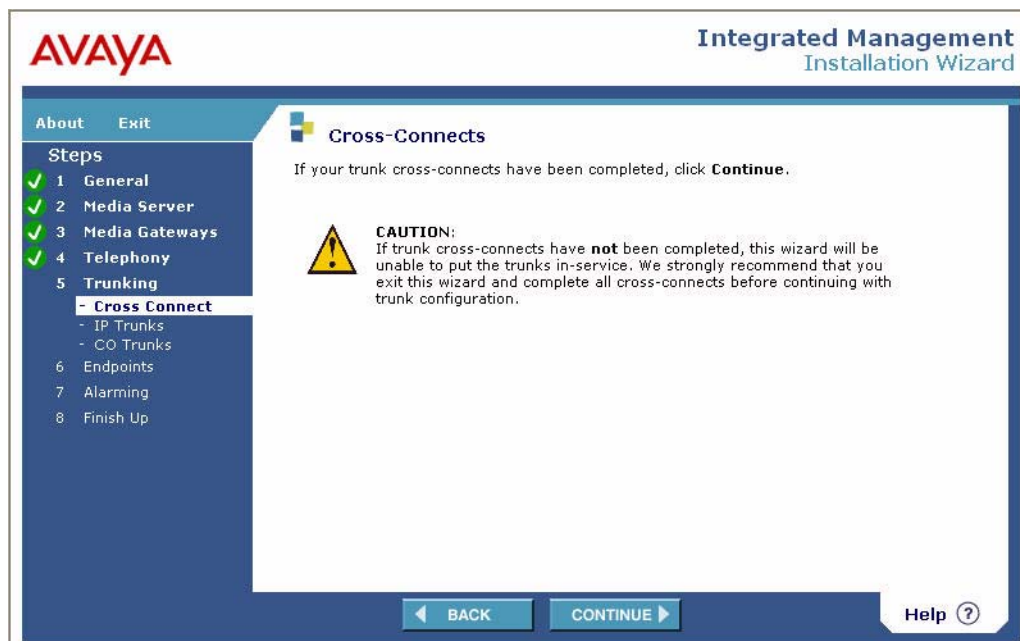
Trunk configuration

For trunk configuration:

1. To configure the G700's trunk parameters, do one of the following:

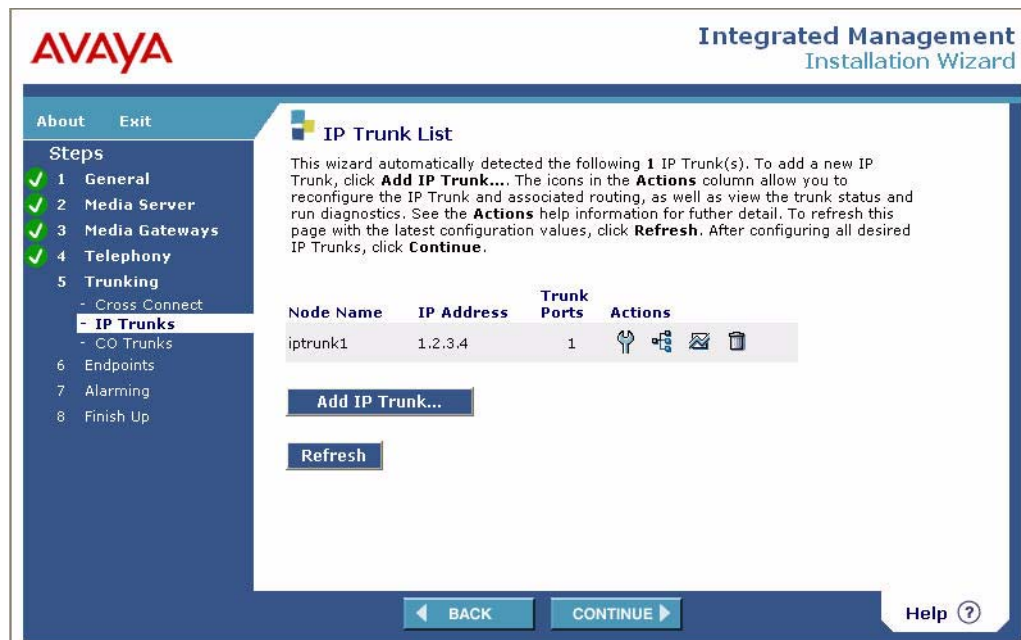
- From the Import Name/Number List screen, click **Continue**, or
- Click **Trunking** from the main menu.

The Cross-Connects screen appears. If your trunk cross-connects have been completed, click **Continue** to proceed with trunk configuration. If your trunk cross-connects have not been completed, it is strongly recommended to exit the Avaya IW and complete all cross-connects before proceeding with trunk configuration.



Installing a new G700 with an S8300 using the Avaya Installation Wizard

2. Click **Continue**. The IP Trunk List screen appears. This screen displays all IP trunks configured on the G700. To refresh this list, click **Refresh**.



3. You can perform the following actions in the IP Trunk List screen:

- [Adding a trunk](#)
- [Modifying trunk parameters](#)
- [Modifying IP route configuration](#)
- [Displaying trunk status](#)
- [Removing a trunk](#)

To proceed to the CO Trunk List screen for configuring a trunk media module, click **Continue**. See [Configuring a trunk media module](#) on page 162.

Adding a trunk

To add a new trunk:

1. Click **Add IP Trunk**. The IP Trunk Configuration screen appears.

The screenshot shows the Avaya Integrated Management Installation Wizard interface. On the left is a 'Steps' sidebar with a tree view containing: 1 General, 2 Media Server, 3 Media Gateways, 4 Telephony, 5 Trunking (with sub-items Cross Connect and IP Trunks), 6 Endpoints, 7 Alarming, and 8 Finish Up. The 'IP Trunks' item is selected. The main area is titled 'IP Trunk Configuration (new)' and contains the instruction: 'Specify the configuration for this IP Trunk. Select the required information and then click **Continue**.' Below this are several input fields: 'Far-End Node Name' (containing 'iptrunk1'), 'Far-End IP Address' (containing '1.2.3.4'), 'Far-End Network Region' (containing '1'), 'Avaya Far-End?' (an unchecked checkbox), 'Number of Trunk Ports' (containing '0' with '(100 Remaining)' text), 'Near-End Listen Port(s)' (containing '0'), and 'Far-End Listen Port(s)' (containing '0'). At the bottom are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

2. Enter the required information in the IP Trunk Configuration screen and click **Continue**. The IP Trunk List appears, with the new trunk included in the list of trunks. To add an additional trunk, click **Add IP Trunk** and repeat this step. When you are finished adding trunks, click **Continue** or select an action from the **Actions** column to modify an existing trunk.

Modifying trunk parameters

To modify the trunk's parameters:

1. Click the configuration icon in the **Actions** column of the IP Trunk List screen.



The IP Trunk Configuration screen appears, with the trunk's current parameters displayed.

The screenshot shows the 'IP Trunk Configuration (iptrunk1)' window within the 'Integrated Management Installation Wizard'. On the left is a 'Steps' sidebar with a tree view: '1 General' (checked), '2 Media Server' (checked), '3 Media Gateways' (checked), '4 Telephony' (checked), '5 Trunking' (expanded, showing 'Cross Connect', 'IP Trunks' (selected), and 'CO Trunks'), '6 Endpoints', '7 Alarming', and '8 Finish Up'. The main area contains configuration fields: 'Far-End Node Name' (iptrunk1), 'Far-End IP Address' (1.2.3.4), 'Far-End Network Region' (1), 'Avaya Far-End?' (checkbox), 'Number of Trunk Ports' (1, with '(100 Remaining)' text), 'Near-End Listen Port(s)' (1719), and 'Far-End Listen Port(s)' (1). At the bottom are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

2. Modify the trunk parameters and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See [Configuring a trunk media module](#) on page 162.

Modifying IP route configuration

To modify the trunk's IP route configuration:

1. Click the IP route icon in the **Actions** column of the IP Trunk List screen.



The IP Route Configuration screen appears.



2. The IP Route Configuration screen displays the extension ranges available for private-network routing. Modify these ranges, if any, and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See [Configuring a trunk media module](#) on page 162.

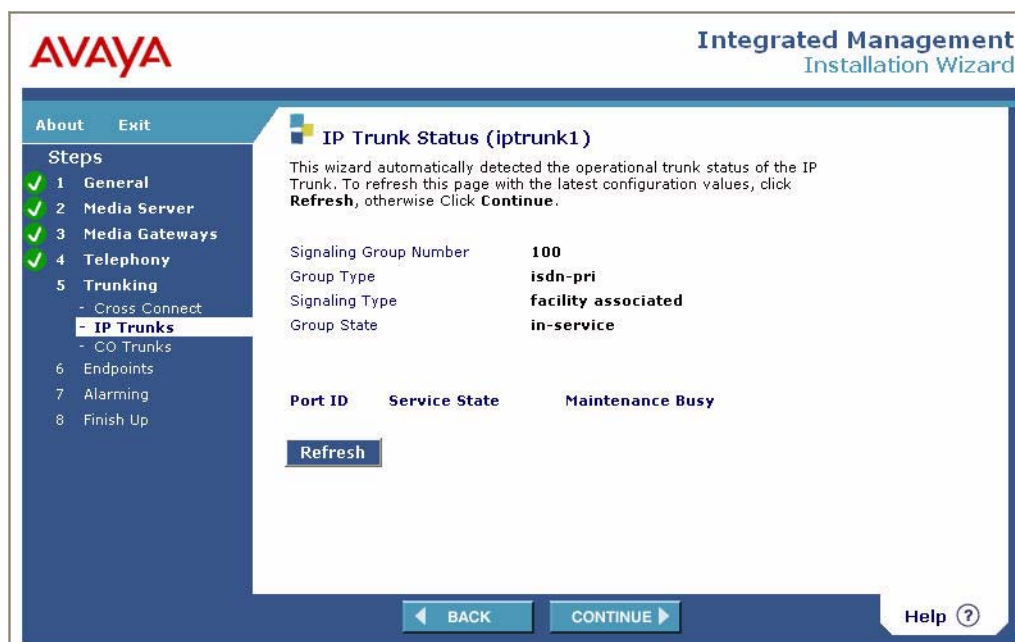
Displaying trunk status

To display the trunk's IP route configuration:

1. Click the trunk status icon in the **Actions** column of the IP Trunk List screen.



The IP Trunk Status screen appears.



2. The IP Trunk Status screen displays the operational status of the trunk. To refresh the information, click **Refresh**. Otherwise, click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See [Configuring a trunk media module](#) on page 162.

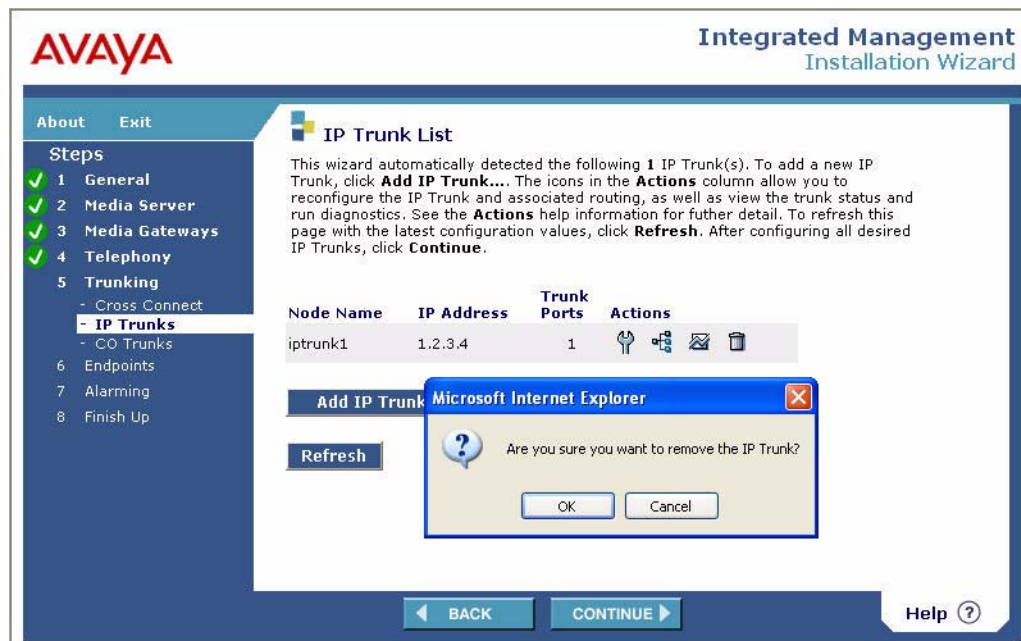
Removing a trunk

To remove a trunk:

1. Click the trunk's remove icon in the **Actions** column of the IP Trunk List screen.



A message appears asking if you want to remove the trunk.



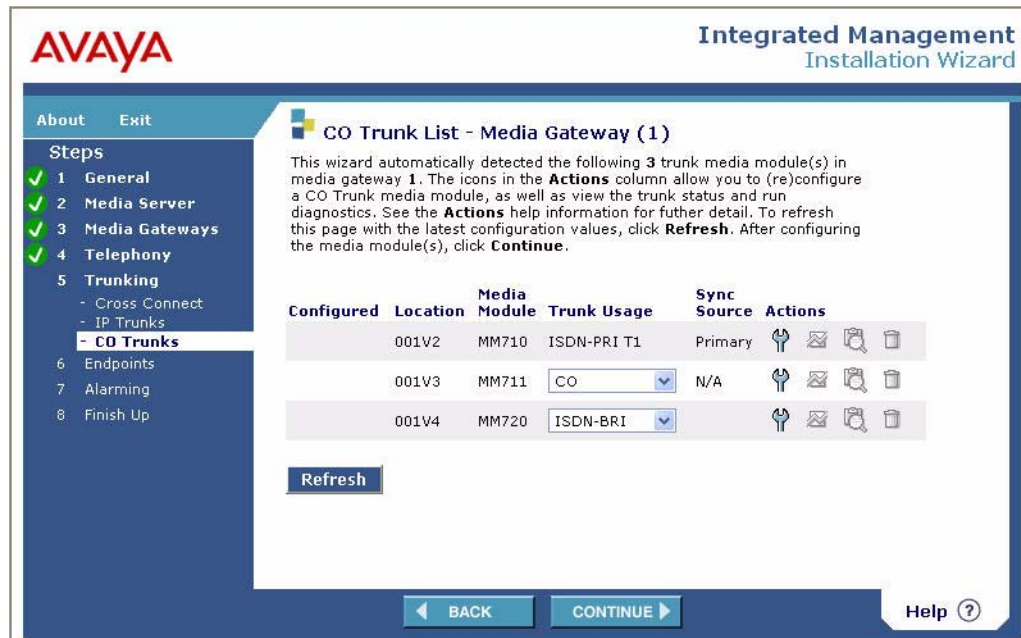
2. Click **OK** to remove the trunk. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen.

Configuring a trunk media module

To configure a trunk media module, do one of the following:

- Click **Continue** from the IP Trunk List screen, or
- Click **Trunking>CO Trunks** from the main menu.

The CO Trunk List screen appears. This screen lists trunk media modules detected in the G700 and allows you to configure a media module and run diagnostics. To configure or run diagnostics on a trunk media module, click the Actions icon for the module.

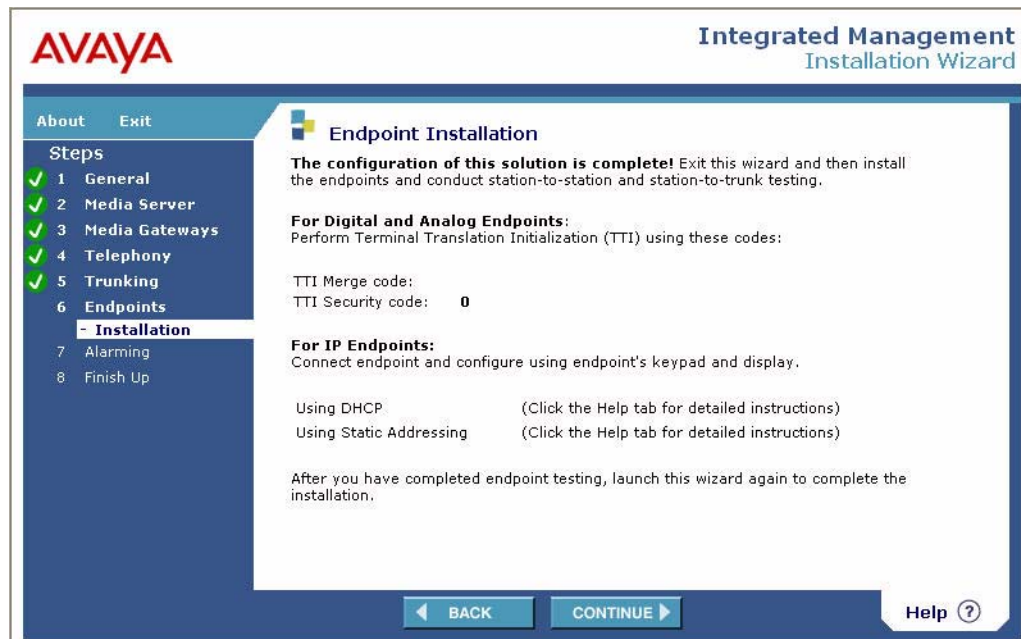


Endpoint installation

For instructions on endpoint installation, do one of the following:

- Click **Continue** from the CO Trunk List screen, or
- Click **Endpoints** from the main menu.

The Endpoint Installation screen appears. You can access endpoint installation information from this screen.



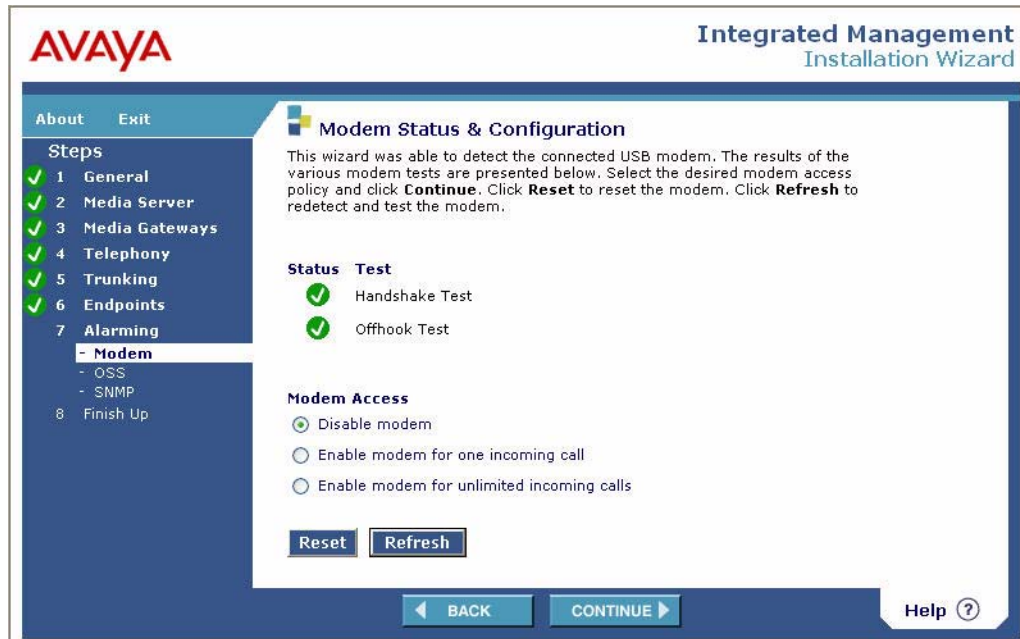
Alarm configuration

To display modem status and configure alarms:

1. Click **Alarming** from the main menu.

The Modem Status & Configuration screen appears. This screen detects any modem connected to the G700. The screen also displays the results of tests performed on the modem. You can perform the following actions from this screen:

- Click **Reset** to reset the modem.
- Click **Refresh** to re-detect and test the modem.



2. Select the appropriate modem access policy in the **Modem Access** area and click **Continue**.

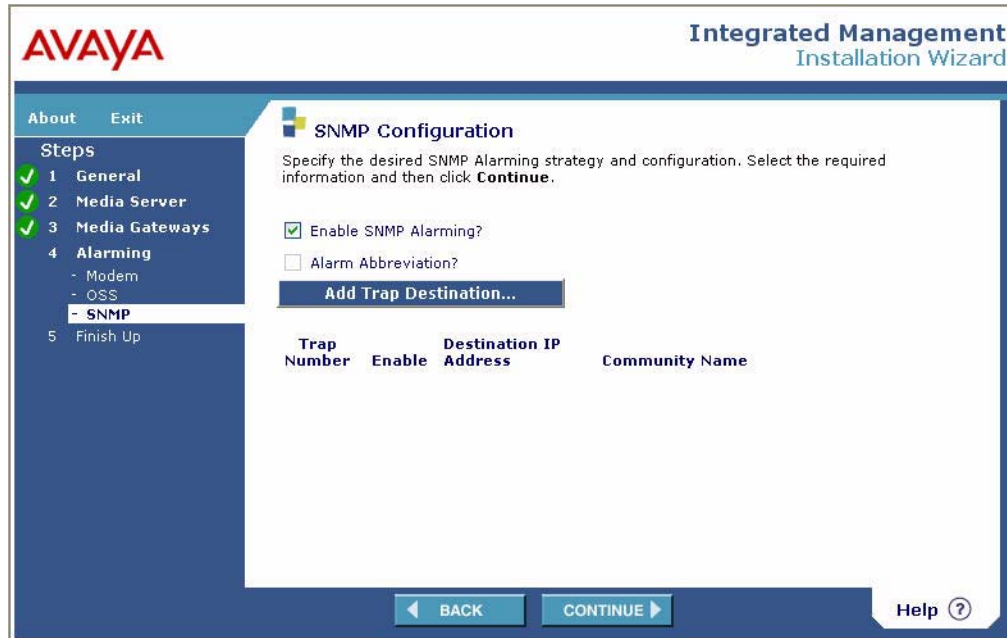
The OSS Configuration screen appears.

The screenshot shows the 'OSS Configuration' screen within the Avaya Integrated Management Installation Wizard. The left sidebar lists the steps: 1 General, 2 Media Server, 3 Media Gateways, 4 Telephony, 5 Trunking, 6 Endpoints, 7 Alarming (with sub-items Modem and OSS), and 8 Finish Up. The 'OSS' sub-item under 'Alarming' is currently selected. The main content area is titled 'OSS Configuration' and includes instructions: 'Specify the desired OSS Alarming strategy and configuration. Select the required information from the **ART tool** and then click **Continue**.' Below this, the 'Alarm Origination' section has three radio button options: 'Neither Phone Number' (selected), 'First Phone Number', and 'Both Phone Numbers'. There are two text input fields for '1st Phone Number' (containing '1234567890') and '2nd Phone Number' (empty). Each input field has a checked checkbox for 'Alarm Abbreviation?'. At the bottom, there are 'BACK' and 'CONTINUE' buttons, and a 'Help' link with a question mark icon.

3. Enter the required information from the ART tool. For information on using the ART tool, see [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 122.
4. Click **Continue**.

The SNMP Configuration screen appears.

5. Check Enable SNMP alarming if you want to enable the sending of SNMP traps to the INADS. In the Destination IP Address field, enter the INADS IP address. In the Community Name field, enter an SNMP community access string. Check the Alarm abbreviation checkbox if you want to enable SNMP alarm abbreviation.

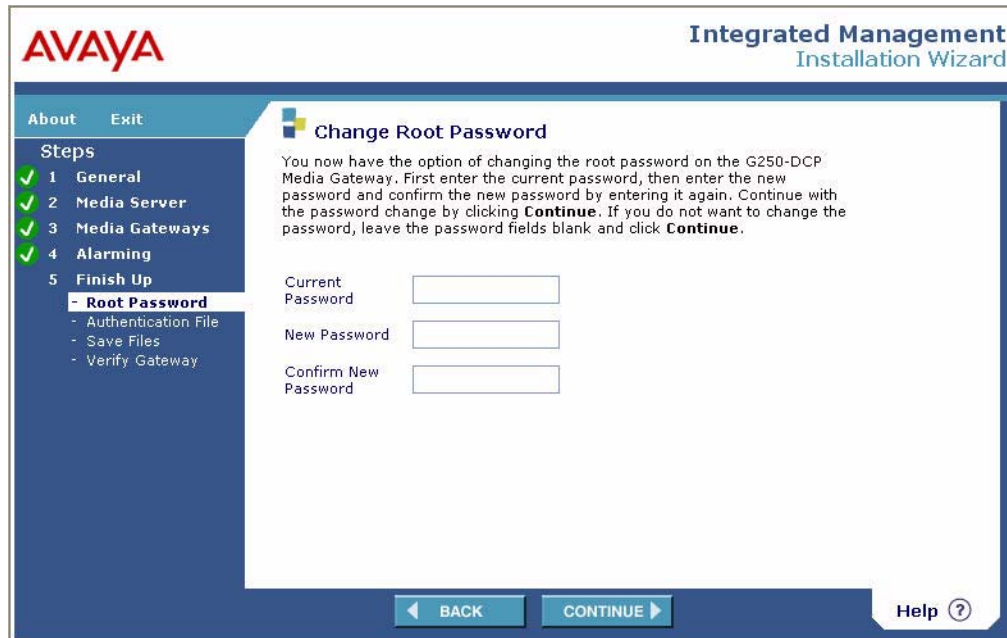


Password and final screens

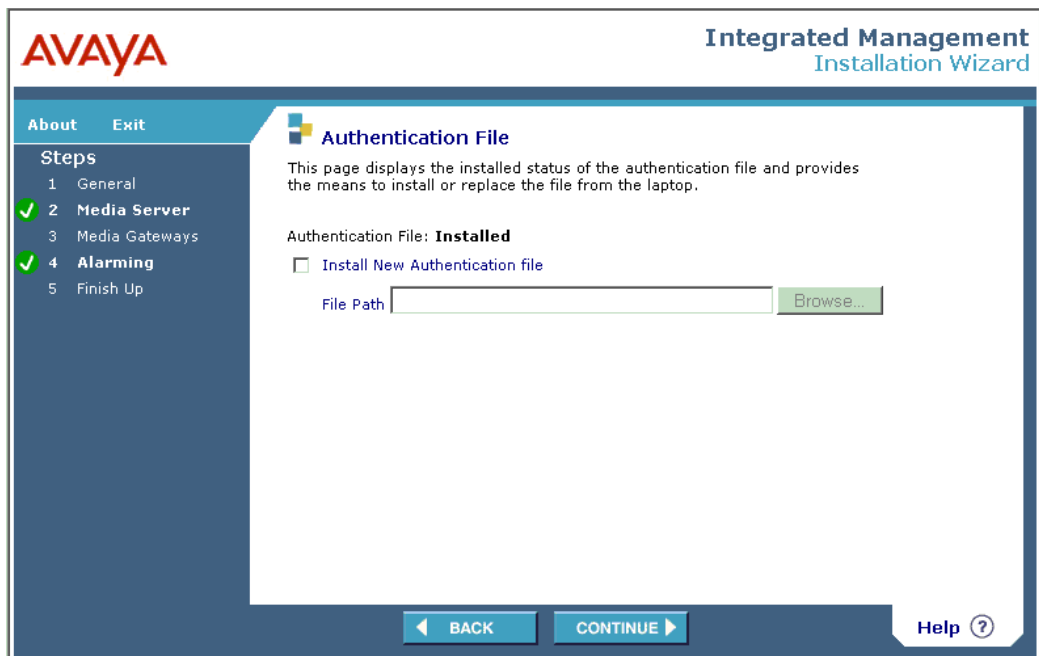
To change your password (optional) and complete the installation:

1. Click **Continue** from the SNMP Configuration screen.

The Change Root Password screen appears. This screen allows you to change the root password on the G700.



2. Click **Continue**.
3. The Authentication File screen appears. This screen allows you to install the authentication file for access to the S8300 Media Server.



4. Click **Install New Authentication File**.
5. Click the **Browse** button to locate the authentication file on your laptop.

6. Click **Continue**.

The Finish Up screen appears. This screen allows you to save the installation log file to your laptop. To save the installation log file:

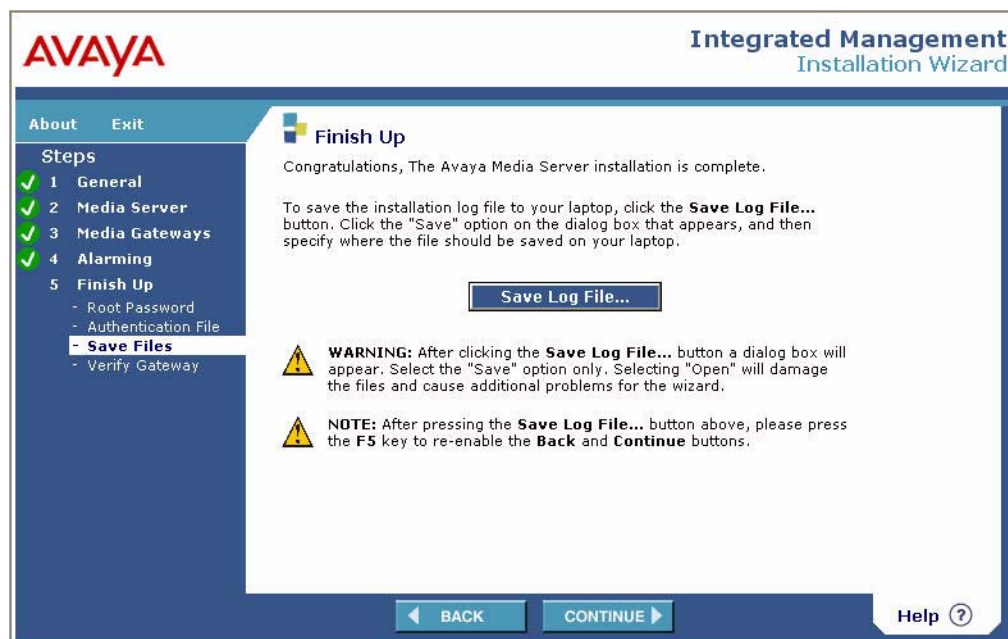
- a. Click **Save Log File**. A dialog box appears.
- b. Click **Save**.



WARNING:

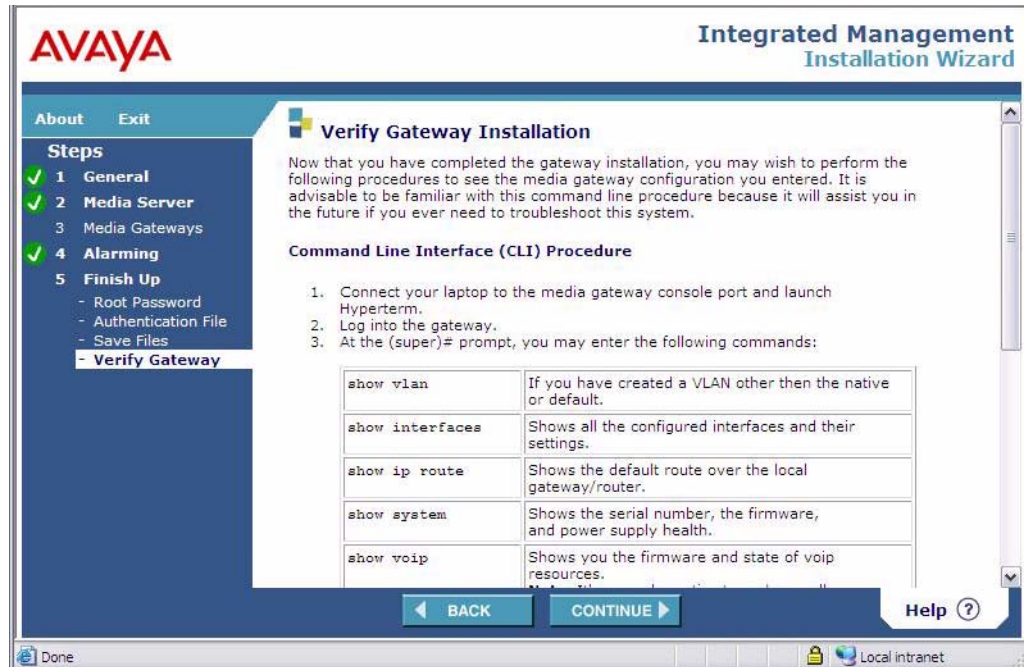
Do not click **Open**. Clicking **Open** will damage the log file and may cause other problems to the Avaya IW.

- c. Press <F5> to restore the **Back** and **Continue** buttons to the Finish Up screen.



7. Click **Continue**.

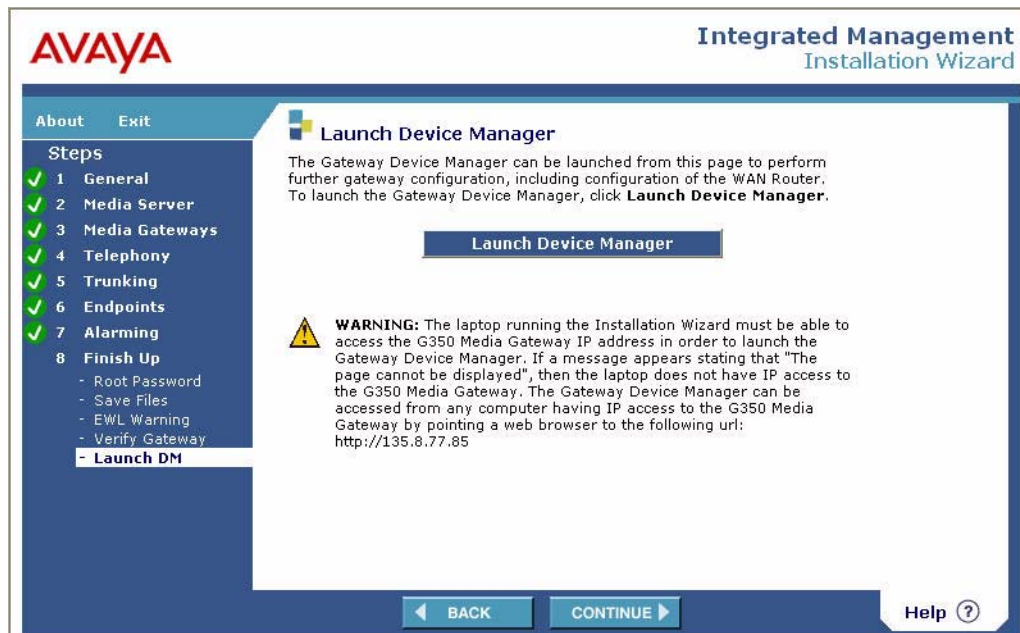
The Verify Gateway Installation screen appears. This screen displays a list of CLI commands that you can use to verify the G700 configuration. The following figure shows a portion of the Verify Gateway Installation screen.



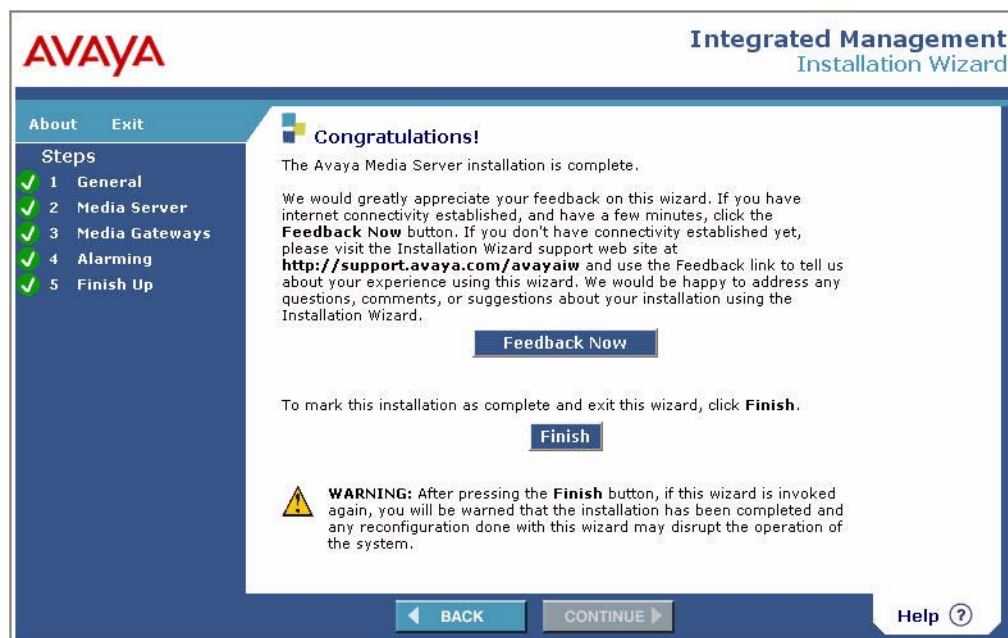
Installing a new G700 with an S8300 using the Avaya Installation Wizard

8. Click **Continue**.

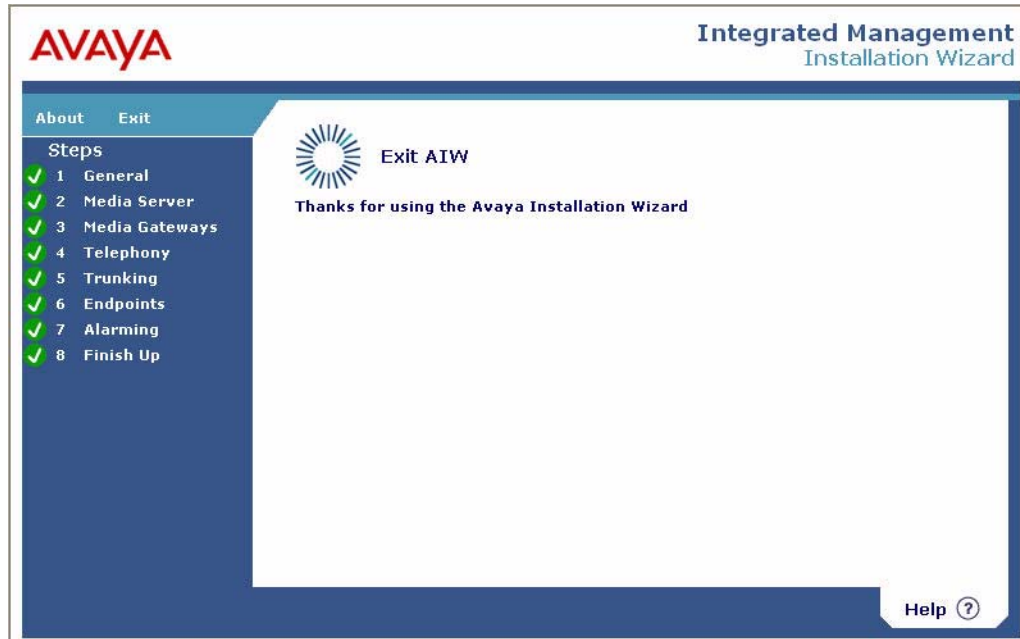
The Launch Device Manager screen appears. This screen allows you to launch the Gateway Device Manager.



9. Click **Continue**. The Congratulations! screen appears to inform you that the installation is complete. To exit the Avaya IW, click **Finish**.



10. The Exit AIW screen appears.



If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`
3. Type `start -ca`

Configuring an X330 Expansion Module (if necessary)

User Guides and Quick Start Guides for the expansion modules are available on the Avaya Support web site:

To obtain the appropriate Avaya Support Web site document

1. Go to the Avaya Support web site: <http://avaya.com/support>.
2. In the list on under Technical Database, click on **LAN, Backbone, and Edge Access Switches**.
3. Under Wiring Closet & Distribution, click on **P330 Stackable Switching**.
4. Click on **All Documents**.
5. Select the appropriate document for the expansion module you are installing.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 Stack Processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 Stack Processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330 Stack Processors now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330T User's Guide* (available at <http://www.avaya.com/support>).

Administering an S8300 primary controller



CAUTION:

This administration applies *only* to an S8300 primary controller, which may be the S8300 Media Server resident in the G700 you are installing or may be an *external* S8300 Media Server somewhere else in the customer's network.

If the S8300 Media Server you just installed is configured as an LSP, do *not* perform this administration on it. Translations are automatically copied to this LSP from the external S8300 primary controller.

Skip this section and go to [Administering an S8400, S8500, or S8700-series primary controller](#) on page 179 if the primary controller is an S8400, S8500, or S8700-series Media Server.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of administration required, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

In this section, you will use the SAT interface to:

- [Assigning Node Names and IP Addresses for the LSPs](#)
- [Administering Network Regions](#)
- [Associating LSPs with Network Regions](#)
- [Administering IP Interfaces](#)
- [Identifying LSPs to the S8300 primary controller](#)



CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the system

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Log in, and open a SAT session (type **sat** or **dsat**).
3. At the SAT prompt, type **reset system 4**
The system reboots.
4. After the reboot is complete, SSH to the S8300, login, and open a SAT session.

Assigning Node Names and IP Addresses for the LSPs

If the S8300 network configuration includes LSPs, they must be specified on the **Node Names** screen.

To assign node names

1. At the S8300 SAT prompt, type **change node-names ip** to open the **Node Names** screen.

Example Node Names Screen

change node-names ip		Page 1 of 1	
IP NODE NAMES			
Name	IP Address	Name	IP Address
default	0__0__0__0__		___.___.___.___
node-10-lsp	192.168.1__50		___.___.___.___
node-11-lsp	192.168.1__51		___.___.___.___
	___.___.___.___		___.___.___.___
	___.___.___.___		___.___.___.___
	___.___.___.___		___.___.___.___

2. Enter the name and IP addresses for the LSPs.
3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 as primary controller, there will usually be one network region, defined as **1**. The procedure below uses 1 for the network region number as an example but the procedure applies for any network region number from 1 to 250.

To define IP network region 1



CAUTION:

Defining IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see “*Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.”

1. At the SAT prompt, type **change ip-network-region 1**.

The S8300 displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain:	
Name:		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 3048		
DiffServ/TOS PARAMETERS		RTCP Reporting Enabled? n
Call Control PHB Value: 34	RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters? y	
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS		RSVP Enabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. If necessary, complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. Press **F3 (Enter)** to submit the screen.

Associating LSPs with Network Regions

If the primary controller has LSPs, you can associate each LSP with one or more network regions. In the event of a network failure, IP telephones assigned to a network region will register with an LSP associated with that region.

This procedure associates up to six LSPs with a network region.

To associate LSPs with a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be associated with region 1.
The LSP names must be the same as administered on the **Node Names** screen.
3. Submit the form.
4. Repeat for each network region with which you want to associate LSPs.

Administering IP Interfaces

This procedure assigns network region 1, as an example, to the S8300 media server.

To assign the network region and IP endpoint access to the S8300

1. At the SAT prompt, type `change ip-interfaces procr.`

The S8300 displays the **IP Interfaces** screen for the media server.

IP Interfaces Screen

```
change ip-interfaces procr                                     Page 1 of 1

                                IP INTERFACES

                                Type: PROCR

                                Node Name: procr
                                IP Address: 135.9.41.146
                                Subnet Mask: 255.255.255.0

                                Enable Ethernet Port? y
                                Network Region: 1
                                Allow H.323 Endpoints? y
                                Allow H.248 Gateways? y
                                Gatekeeper Priority: 5
```

2. The field **Enable Ethernet Port?** should indicate *y* (yes). The **Node Name** should be the IP address of the S8300 media server.
3. In the **Allow H.323 Endpoints** field, enter a 'y' to allow H.323 endpoint connectivity to the server.
4. In the **Allow H.248 Endpoints** field, enter a 'y' to allow H.248 media gateway connectivity to the server.
5. In the **Gatekeeper Priority** field, enter a value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to *y*.

Identifying LSPs to the S8300 primary controller

If the primary controller has LSPs, you must enter the LSP node names on the Survivable Processor form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the **LSP** screen, their status can be viewed with the `list survivable-processor` command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **Survivable Processor** screen.

1. At the SAT command line, type `add survivable-processor <name>`, where *<name>* is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 17: Add Local Survivable Processor screen

add survivable-processor sv-mg2-lsp	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET	
Node Name: sv-mg2-lsp	
IP Address: 128.256.173.101	
Type: LSP	
Network Region: 1	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Skip to [Administering the Media Gateway](#) on page 189.

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

In this case, the S8300 you have installed is configured as an LSP.

**CAUTION:**

This administration applies only to the primary controller that controls the S8300 LSP that you are installing. The primary controller can be an S8400, S8500, or S8700-series Media Server. Do *not* administer the S8300 LSP. Translations are automatically copied to the LSP from the primary controller.

Skip this section and go to [Administering an S8300 primary controller](#) on page 174 if the primary controller is an S8300.

Note:

Some of the procedures in this section may have been completed previously as part of a normal media server installation.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of required administration, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

In this section, you will use the SAT interface on the primary controller to:

- [Assigning Node Names and IP Addresses for the C-LANs and LSPs](#)
- [Administering Network Regions](#)
- [Assigning LSPs to the Network Regions](#)
- [Administering IP Interfaces](#)
- [Identifying the Survivable Processor on the primary controller](#)

Note:

For information on installing the CLAN boards on the S8400, S8500, or S8700-series port networks and complete information on installing an S8400, S8500, or S8700-series Media Server, see the Installation documentation on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

Assigning Node Names and IP Addresses for the C-LANs and LSPs

Note:

The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the media server. For information on how to upgrade the firmware on the S8400, S8500 or S8700-series Media Server, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Media Servers and Gateways*, 03-300412.

To assign node names and IP addresses

1. At the SAT prompt, type `change node-names ip` to open the **Node Names** screen.

Example Node Names Screen

change node-names ip		Page 1 of 1	
IP NODE NAMES			
Name	IP Address	Name	IP Address
default_____	0__0__0__0__	_____	____.____.____.____
node-1-clan_____	192.168.1__124	_____	____.____.____.____
node-2-clan_____	192.168.1__97	_____	____.____.____.____
node-10-lsp_____	192.168.1__50	_____	____.____.____.____
node-11-lsp_____	192.168.1__51	_____	____.____.____.____
_____	____.____.____.____	_____	____.____.____.____
_____	____.____.____.____	_____	____.____.____.____
_____	____.____.____.____	_____	____.____.____.____

2. Enter the name and IP address for the C-LANs and LSPs.
3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 LSP and an S8500 or S8700-series Media Server as the primary controller, there may be more than one network region, since there can be up to 250 G700 media gateways connected to the S8500 or S8700-series Media Server with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700-series port networks, though they may also have the same network region.

Note:

With an S8300 or an S8400 Media Server, there still may be a need for more than one network region, though the S8400 supports up to five media gateways and the S8300 supports up to 50 media gateways.

The G700, in the case of multiple network regions, may also share the same network region as the CLAN board(s). However, it may have a different network region because of the geographic distances of the connections between the G700 and the primary controller. The G700 network region may also differ because of the nature of the endpoints connected to it.

To configure IP network regions for the G700 and CLAN board(s)



CAUTION:

Configuring IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

1. On the SAT screen of the primary controller for the G700 media gateway, type **change ip-network-region <network_region>**

where **<network_region>** is the region you will assign to the G700 media gateway. This region number may or may not match the network region of the S8400, S8500, or S8700-series CLAN boards.

The system displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain:		
Name:		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? y
UDP Port Max: 3048		
DiffServ/TOS PARAMETERS		RTCP Reporting Enabled? n
Call Control PHB Value: 34		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? y
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. Complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. If the network region of the G700 (1 in this example) is different from that of the S8400, S8500, or S8700-series CLAN board(s), you must interconnect the two regions.

Press **NextPage** twice to display page 3, of the **Inter Network Region Connection Management** screen.

This screen shows the source region (1) and the first 15 destination network region numbers. (Pages 4–19 show destination regions 16–250).

IP Network Region Screen, Page 3

display ip-network-region 1									
Inter Network Region Connection Management									
src	dst	codec	direct				Dynamic	CAC	
rgn	rgn	set	WAN	WAN-BW-limits	Intervening-regions		Gateway		IGAR
1	1	1							
1	2								
1	3								
1	4								
1	5								
1	6								
1	7								
1	8								
1	9	3							
1	10								
1	11								
1	12								
1	13								
1	14								
1	15								

4. Type the number for the type of codec set (1–7) that the S8400, S8500, or S8700-series Media Server will use to interconnect the G700 and the C-LAN board(s) in the row corresponding to the region of the C-LAN.

In this example, the C-LAN is in region 9 and codec-set type 3 is to be used for the interconnection between region 1 and region 9. (In this example, codec type 1 is used for communication within region 1)

The SAT command, **list ip-codec-set**, lists the types of codecs available on this server.

For more detail about the Inter Network Region Connection Management form, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

5. Press **F3 (Enter)** when complete.

Assigning LSPs to the Network Regions

If the primary controller has LSPs, you can assign the LSPs to network regions. In the event of a network failure, IP telephones assigned to a network region will register with the LSPs assigned to that region.

This procedure assigns up to six LSPs to a network region.

To assign LSPs to a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1

Page 2 of 19

IP Network Region

INTER-GATEWAY ALTERNATIVE ROUTING

Incoming LDN Extension:

Conversion To Full Public Number - Delete: Insert:

Maximum Number of Trunks to Use:

LSP NAMES IN PRIORITY ORDER

1 node-10-LSP_____

2 _____

3 _____

4 _____

5 _____

6 _____

SECURITY PROCEDURES

1 challenge

2 _____

3 _____

4 _____

2. Enter the names of up to six LSPs to be assigned to region 1.
The LSP names must be the same as administered on the **Node Names** form.
3. Submit the form.
4. Repeat for each network region to which you want to assign LSPs.

Administering IP Interfaces

To define the IP interfaces of the S8400, S8500, or S8700-series port network CLAN boards

Note:
This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type `change ip-interfaces <slot location>` to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces 01A03	Page 1 of 1
IP INTERFACES	
Type: C-LAN	
Slot: 01A03	
Code/Suffix: TN799 d	
Node Name: CLAN1	
IP Address: 135.9.41.146	
Subnet Mask: 255.255.255.0	Link: 1
Gateway Address: 135.9.41.254	
Enable Ethernet Port? y	Allow H.323 Endpoints? y
Network Region: 1	Allow H.248 Gateways? y
VLAN: 0	Gatekeeper Priority: 5
Target socket load:	
Receive Buff TCP Window Size:	
ETHERNET OPTIONS	
Auto? n	
Speed: 100 Mbps	
Duplex: Full	

2. Complete the fields as described the in [Table 8](#).

Table 8: IP interfaces field descriptions

Field	Conditions/Comments
Type	Either C-LAN.
Slot	The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799 for C-LAN.
Node name	The unique node name for the IP interface. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the C-LAN.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see “ <i>Administration for Network Connectivity for Avaya Communication Manager, 555-233-504</i> ”.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.

1 of 2

Table 8: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
VLAN	The VLAN number assigned to the C-LAN, if any.
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Receive Buffer TCP Window Size	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.
Link	This display only field shows the unique number for the Ethernet link. The Ethernet link was assigned on the data module form.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
Auto?	Enter 'y' or 'n' to set auto-negotiation.
Speed	Enter 10 or 100 Mbps if Auto was set to no.
Duplex	Enter half or full if Auto was set to no.

2 of 2

3. Close the screen.

To define the IP interface of the S8400 or S8500 processor Ethernet port**Note:**

This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type `change ip-interfaces procr` to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces procr		Page 1 of 1
IP INTERFACES		
Type: PROCR		
Node Name: procr		
IP Address: 135.9.41.146		Link: 1
Subnet Mask: 255.255.255.0		
Enable Ethernet Port? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
Target socket load:		

2. Complete the fields as described the in [Table 9](#).

Table 9: IP interfaces field descriptions

Field	Conditions/Comments
Type	Display only. PROCR
Node name	The unique node name for the IP interface. procr is the default node name. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the Processor Ethernet.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see <i>“Administration for Network Connectivity for Avaya Communication Manager, 555-233-504”</i> .
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.

1 of 2

Table 9: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.

2 of 2

3. Close the screen.

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the LSP form, their status can be viewed with the `list survivable-processor` command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

1. At the SAT command line, type `add survivable-processor <name>`, where `<name>` is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 18: Add Local Survivable Processor screen

<pre>add survivable-processor sv-mg2-lsp</pre>	Page 1 of xx
<pre>SURVIVABLE PROCESSOR - PROCESSOR ETHERNET</pre>	
<pre>Node Name: sv-mg2-lsp</pre>	
<pre>IP Address: 128.256.173.101</pre>	
<pre>Type: LSP</pre>	
<pre>Network Region: 1</pre>	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Administering the Media Gateway

To perform the procedures in this section, to the primary controller, log in, and open a SAT session.

**CAUTION:**

Before administering a media gateway, make sure that the gateway has been fully configured.

In this section, you will do the procedures:

- [To add a media gateway](#)
- [To verify changes](#)
- [To enable announcements, if necessary](#)

To add a media gateway

1. At the SAT prompt, type `add media-gateway <number>`

where *<number>* is the gateway number from 1 to *n*. (*n* is 50 for an S8300, 5 for an S8400, and 250 for an S8500 or S8700-series Media Server).

The S8300 displays the **Media Gateway** screen.

Add media gateway Screen

add media-gateway 1

Page 1 of 1

MEDIA GATEWAY

Number: 1

Type: g700

Name: Swainsons

Serial No: 012X06230551

Encrypt Link? y

Network Region: 1

Location: 1

Recovery Rule: none

Registered:

FW Version/HW Vintage:

IP Address:

Controller IP Address:

MAC Address: 00:04:0d:02:06:ca

CF: 8 MB

Site Data:

Slot	Module Type	Name
V1:		
V2:		
V3:		
V4:		
V9:		

2. Complete the **Name** field with the hostname assigned to the G700 media gateway.
3. Complete the **Identifier** field with the serial number of the G700 media gateway.

You can obtain the serial number by typing the **show system** command at the MGP command line interface.

CAUTION:

Be sure the serial number for the G700 media gateway you enter in this procedure matches *exactly* the serial number displayed in the **show system** command. The serial number is case-sensitive, and if entered incorrectly, will prevent the S8300 media server from communicating with the G700 media gateway.

4. Complete the **Network Region** field with the value supplied in the planning documentation.
5. If specifically requested by the customer or your planning documents, type **gateway-announcements** in the V9 field.

This field allows you to enable announcements on the G700 media gateway. V9 is a virtual slot. There is no announcement board associated with it. The announcements for the G700 are available in the G700 firmware and are administered in the same way as announcements on the TN2501 circuit pack used on S8400, S8500, or S8700-series port networks.

If there are multiple G700 media gateways sharing announcements, then enable announcements on the G700 whose trunks will receive the announcements most often.

6. Press **F3 (Enter)** to save your changes.

If properly administered, the G700 should register with the primary controller within 1–2 minutes. The **IP Address**, **MAC Address**, and **Module Type** fields are populated automatically after the G700 media gateway registers with the server.

7. Type **change media-gateway** to view the **Media Gateway** screen.

Media Gateway screen (after registration with primary controller)

```

change media-gateway 1                                     Page 1 of 1

                                MEDIA GATEWAY

      Number: 1                      Registered: y
      Type: g700                    FW Version/HW Vintage: 21.13.0 /0
      Name: Swainsons                IP Address: 135.9.41.150
      Serial No: 012X06230551        Controller IP Address: 135.9.41.146
Encrypt Link? y                      MAC Address:
Network Region: 1                      CF: 8 MB
      Location: 1                      Site Data:
Recovery Rule: none

Slot  Module Type      Name
V1:   S8300            ICC MM
V2:   MM712            DCP MM
V3:   MM711            ANA MM
V4:   MM710            T1/E1 MM

V8:
V9:
  
```

The media modules installed in the G700 are listed next to their slot numbers. Verify that a G700 media gateway has been successfully added.

To verify changes

1. At the SAT prompt, type **list media-gateway**.

Media-Gateway Report screen

```

list media-gateway

                                MEDIA-GATEWAY REPORT
  
```

Number	Name	Serial No/ FW Ver/HW Vint	IP Address/ Cntrl IP Addr	Type	NetRgn RecRule	Reg?
1	LabA	01DR07128730 21 .13 .0 /0	135.177.49.57 135.177.49.59	g700	1 1	y
2	Data MG2	02DR01130356 11 .2 .0 /0	135.177.49.90 135.177.49.40	g350	1 none	n

2. Verify that the G700 media gateway has registered.

The `y` in the registered field signifies that the G700 media gateway has registered. If the G700 should become unregistered, the `y` will become an `n`, but the IP address will remain assigned to the G700 media gateway. If the G700 has never been registered, the IP Address field will be blank.

If the G700 fails to register, two common causes are:

- The serial number added as the **Identifier** for the G700 is wrong. To check, log back into the G700 gateway and type `show system`. Check the serial number that appears.
- There is no IP connection between the G700 and the S8300. To check, type `show mgc` and then `ping mgp <controller_address>`.

To enable announcements, if necessary

1. *Only if specifically requested by the customer or your planning documents*, at the SAT prompt, type `enable announcement-board <gateway_number> v9`

where `<gateway_number>` is the number of the G700 media gateway you added.

`v9` is the virtual slot (for example, `2v9` means media gateway number 2, slot V9).

2. Press **Enter** to enable announcements.

The system displays the message

Command successfully completed

Saving Communication Manager translations

Save translations again after all Communication Manager administration is complete.

1. At the SAT prompt, type `save translation`

Considerations for IP Phones Supported by a Local Survivable Processor

A DHCP server assigns IP addresses to IP endpoints dynamically. Avaya IP phones perform a DHCP discover request to receive an IP address, as well as receive parameters necessary to function correctly. These parameters include the location of the call control server, the location of the TFTP server, as well as the directory on the TFTP server from which the phone receives its upgrades.

When preparing a DHCP server to work with Avaya IP phones, there is an option that must be administered to allow the Avaya phone to receive the DHCP offer. This option is "site-specific-option-number" (sson) 176. Different DHCP servers allow for this administration in different ways, but the sson option must be mapped to 176. Then the option can be set up to send the information desired to the Avaya phones for the intended activity.

The sson option sends a string that includes the IP address of the Avaya Call Controller with which the phone will register ("MCIPADD=www.xxx.yyy.zzz"). In an S8400, S8500, or S8700-series system, this can be a CLAN address; in an S8400 or S8500, this can also be the IP address for the server's port that is enabled for processor ethernet; in an S8300 system, this is the IP address of the S8300. Multiple addresses can be administered to allow for LSP failover. The second address in the MCIPADD list may be an IP address for a second CLAN board or an LSP. If a second CLAN board is used, then the third address must be the LSP, and any subsequent addresses should be alternate LSPs. Local LSPs should appear first in the list, with remote LSPs later in the list as possible back ups.

If an IP phone loses its connection to the primary controller, it will try to register with an LSP associated with its network region (as defined on page 3 of the IP Network Region form). However, if the phone resets, it loses this information and goes to the DHCP server for a controller. If the only controller in the MCIPADD list is the primary controller, and if the connection to the primary controller is down, the phone cannot register. Having an LSP in the MCIPADD list gives the IP phones an alternate controller in this situation.

Note:

It is strongly recommended that at least one LSP be administered in the MCIPADD list.

Also included in the sson option string is the "MCPORT=1719". This is the port the phone will listen on for signalling traffic to the call controller. Next is the tftp server field. This field indicates to the phone where it is to receive firmware updates, along with the tftp directory field.

Note:

See *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507, for information about IP Telephones.

All phones for which the DHCP server has an LSP as the second address in the MCIPADD list should be administered to be in the same network region. Or, if administered to be in different network regions, the network regions involved should be interconnected. Use the ip-network-map form on the primary controller to put the IP phones in the same network region. On the ip-network-map form, a range of IP addresses (or a subnet) can be specified to be in a single network region. Enter the IP address range, or subnet, that contains the IP addresses of the IP phones and enter the desired network region number for that address range. The same address range or subnet must then be administered on the DHCP server. If it is not desired that all the phones be in the same network region, the form “ip-network-region #” should be used to interconnect all the network regions that contain those phones.

Transition of Control from Primary Controller to LSP

When the network connection between the G700 and the S8300, S8400, S8500, or S8700-series primary controller goes down, control of endpoints connected to the G700 goes to the next point in the primary controller list, which will be either a second CLAN board (when used with the S8400, S8500, or S8700-series) or an LSP. At this point, the primary controller alarms to notify the customer and services personnel that the network connection between the primary controller and G700 has problems. If control passes to the LSP, the LSP's license allows it to support the G700 endpoints for up to 30 days, within which the network problems should be resolved.

The customer may pass control back to the S8300, S8400, S8500, or S8700-series primary controller manually, by selecting **Shutdown this server** from the S8300 LSP web page (includes selecting the option to restart after shutdown), or a technician must run **reset system 4** from the SAT command line from the S8300 LSP. When the system reboots, the G700 and its endpoints reregister with the primary controller.

The customer may also choose to administer Communication Manager on the System Parameters Media Gateway Automatic Recovery Rule screen, such that the primary controller accepts control back from the LSP as soon as possible, based on whether there are calls active or what time of day it is. See *Administrator Guide for Avaya Communication Manager*, 03-300509.

Complete the Installation of the S8300 (if the Primary Controller)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test the endpoints
- Administer Communication Manager for trunks, features, networking, or other items required by the customer
- Complete the electrical installation
- Enable adjunct systems

Note:

Follow the existing process and procedures to register the S8300.

Updating IA770 INTUITY AUDIX Messaging, if installed

Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update

After the upgrade is complete, perform the following post-upgrade tasks.

2. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

3. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

4. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

5. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing IA770 service pack (or RFU) files, if any

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at <http://support.avaya.com>.

1. Select **Messaging Administration** from the main menu.
2. Select **Utilities** from the Messaging Administration menu.
3. Select **Software Management** from the Utilities menu.
4. Select **Advanced Software Installation** from the Software Management menu.
5. Select **Continue this operation without current system backup**.
6. Select the IA770 update package and click **Install Selected Packages**.

Note:

The system automatically prompts you to restart INTUITY AUDIX when the service pack has been installed. Therefore, if you restart AUDIX at this time, you do *not* need to perform the following procedure, [Starting IA770 INTUITY AUDIX Messaging](#).

Starting IA770 INTUITY AUDIX Messaging

 CAUTION:

You do *not* need to perform this task if you restarted AUDIX as a part of the installation of the IA770 service pack.

After the IA770 INTUITY AUDIX Messaging application has been updated, you must restart it using the following steps:

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Start Messaging Software**.

The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Verifying start up of IA770 INTUITY AUDIX Messaging

To verify operation of IA770 INTUITY AUDIX Messaging, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.
the **View Process Status Results** screen displays.

View Process Status screen



Process Name	Count	Status
Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAlarmAgen	1/ 1	UP
C3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

Help

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an IA770 sanity test:
 - a. At the Linux command line, type `/vs/bin/display`
 - b. All states should be `Inserv` with an associated phone number.
 - c. Retrieve the test message saved before the upgrade.

If IA 770 fails to start after a new installation

If you have installed or upgraded IA 770 INTUITY AUDIX and it does not start, you must ensure that an IP address has been provided for use with IA 770. To check for the IP address, you must use the **Configure Server** option through the Maintenance Web pages.

On the Configure Interfaces screen, ensure that a valid IP address is present in the **Integrated Messaging** section.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **save translation** and press **Enter**.

When the save is finished, the system displays the message,

`Command successfully completed.`

Backing up the system

To back up the system to compact flash media (S8300C Media Server only)

1. Plug the cable to the compact flash drive into a USB port on the S8300C.
2. Insert a 128-Mb compact flash media into the top right slot of the drive.
3. On the S8300 main menu, select **Backup Now**.

The system displays the **Backup Now** screen.

4. Select the type of data you want to back up by selecting the appropriate data set.
5. Select **Local Compact Flash Card** back up the data onto the compact flash card.

Optionally, select Format Compact Flash to format a new card.

Note:

The compact flash card needs to be formatted only before the first use.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

To back up the system over the customer's LAN

1. Make sure you have the IP address of the customer's FTP, SFTP, or SCP backup server.
2. On the S8300 main menu, select **Backup Now**.

The system displays the **Backup Now** screen.

3. Select the type of data you want to back up by selecting the appropriate data set.
4. Select a backup method, normally **FTP**, **SFTP**, or **SCP**, to indicate the destination to which the system sends the backup data.
5. Complete the following fields:

- **User name**

You must enter a valid user name to enable the media server to log in to the FTP or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.

- **Password**

You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.

- **Host name**

Enter the DNS name or IP address of the FTP or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

- **Directory**

Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. The default directory for backup data on the FTP or SCP server is /var/home/ftp. If you do not want to use the default directory, you must enter the path name for the directory.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

This completes the installation of the G700 Media Gateway with an S8300 Media Server as primary controller.

If using IA770, administer Communication Manager for Integrated Messaging

A number of administration tasks must be performed to allow IA770 Integrated Messaging to work. These tasks are explained in detail in *Administering Media Servers to work with IA770*.



CAUTION:

IA770 INTUITY AUDIX Messaging processes messages using the G.711 codec only. Therefore, ensure that a codec set exists that uses only the G.711 codec. Then, assign that codec set to a network region. And, finally, assign that network region to the AUDIX signaling group that is linked to the IA770 INTUITY AUDIX Messaging trunk group.

Complete the Installation Process (for an S8300 LSP)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test endpoints
- Complete the electrical installation
- Enable adjunct systems

This completes the installation of the G700 Media Gateway with an S8300 LSP.

Chapter 4: Installing a new G700 without an S8300 using the Gateway Installation Wizard

This chapter covers the procedures to install a new Avaya G700 Media Gateway without an Avaya S8300 Media Server. The G700 is controlled by an external primary server running Avaya Communication Manager. The primary server can be an S8400, S8500, or S8700-series Media Server or an S8300 residing in another G700.

Note:

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

The Avaya Gateway Installation Wizard (GIW) performs these tasks automatically

- Assigning the IP addresses of the G700 media gateway components
 - Assigning the IP address for the P330 Stack Processor
 - Establishing IP routing for the stack
 - Assigning the IP address to the G700 media gateway processor
 - Assigning the default IP route to the G700 media gateway
 - Assigning IP addresses to the VoIP resources
 - Checking for IP connections
- Setting up the media gateway controller list
- Setting the Link Loss Transition Points

However, the GIW does *not* configure an X330 Expansion module. This task you must still perform manually, as described in:

- [Configure an X330 Expansion Module \(If Necessary\)](#)

Installation overview

What are the system components

About G700 components

A P330 Stack Processor is built into the G700 Media Gateway. (This processor is also known as the *Layer 2 switching processor*). In addition, the G700 contains:

- Media Gateway Processor (MGP)
- VoIP processor
- Up to four media modules
- Possibly an expansion module

Installing or upgrading the firmware for one or more of these processors and/or media modules is a required part of most new installations or upgrades.

About firmware files

You should obtain the firmware files for the G700 before going on-site. You can obtain the firmware files in bundled form on a CD or you can go to the Avaya Support website and download the individual firmware files onto your services laptop.

About the TFTP server

To install firmware on a G700 without an S8300 or LSP, you must first copy the firmware files to an external TFTP server on the customer LAN. The TFTP server can be a customer computer or it can be set up on your services laptop.

What provides initial access to the G700

Before the P330 stack processor is configured with an IP address, the only way to access it is with a direct connection from your laptop to the Console port on the G700. With this connection, you can assign the IP addresses to the G700 processors, which can then be accessed over the customer LAN.

Before going to the customer site

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

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Installing the Gateway Installation Wizard

To obtain and install the GIW software

1. Go to <http://support.avaya.com/avayaiw>.
2. Click on **Download Gateway Installation Wizard (GIW)**.
3. Scroll down to the GIW program file, and click on the latest filename (for example, **GIW-4.0-1.exe**).
4. Save it to a directory on your laptop.
5. Click on the GIW Readme file (for example, **GIW-4.0-1.README**).
6. Save this file to your laptop.
7. Follow the instructions in the Readme file to install the GIW.

Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary

A tar.gz file, which you obtain from a CD-ROM or a website, contains new G700 firmware. To load the firmware on a G700 Media Gateway, you must place this tar.gz file on a TFTP server that is connected to the customer's LAN. The TFTP server can be a customer computer or it can be your laptop if you have arranged with the customer to connect your laptop to the LAN.

Note:

A Linux or Unix TFTP server should be used only if the customer already has an existing one. In these cases, you download the tar.gz file to your laptop and give it to the customer for proper placement and execution.

To obtain the TFTP server software and install it, see [Appendix D: Install the Avaya TFTP server](#).

Downloading G700 firmware files to your TFTP directory

To install new firmware for the G700 processors and the media modules, you first need to move the new firmware files to a directory on the TFTP server. The installation program reads the new firmware files from this directory on the TFTP server.

Perform one of the two procedures in this section, depending on whether you have a bundled tar.gz file on a CD or wish to download individual firmware files from the Avaya Support website.

Downloading individual firmware files

Download the firmware files from the Web to your TFTP directory

Note:

The sequence of links on the website may be somewhat different than described here.

1. Access the <http://www.avaya.com/support> website.
2. Navigate to Firmware Downloads for The G700 Media Gateway.

The system displays a list of firmware files.

3. Locate the file names that match the files listed in your planning documentation.

The file names will approximate those listed in [Table 10](#).

Note:

The latest firmware versions may differ from those listed in [Table 10](#). Also, the appropriate firmware version may depend on the hardware vintage and/or on the release of Communication Manager. See *Communication Manager Software/Firmware Compatibility Matrix* under Downloads on support.avaya.com.

**CAUTION:**

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Table 10: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_1_6.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.6.6.exe
G700 Media Gateway	mgp<version id>	mgp_24_21_1.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v57.fdl
8-port DCP Media Module	mm712<version id>	mm712v7.fdl
24-port analog Media Module	mm716<version id>	mm716v2.fdl
24-Port DCP Media Module	mm717<version id>	mm717v4.fdl
8-port/trunk Analog Media Module (version 6 or earlier)	mm711<version id>	mm711v17.fdl
8-port/trunk Analog Media Module (version 7)	mm711<version id>	mm711h7v24.fdl
8-port/trunk Analog Media Module (version 20 or later)	mm711<version id>	mm711h20v68.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v67.fdl
T1/E1 Media Module	mm710<version id>	mm710v14.fdl
8-port BRI Media Module	mm720<version id>	mm720v6.fdl
2-port BRI Media Module	mm722<version id>	mm722v2.fdl

- Double-click the file name.

The system displays a **File Download** window.

- Click on **Save this file to disk**.
- Save the file to the **C:\tftp** directory (or your alternate tftp location).
- Use WinZip or another zip file tool to unzip the file, if necessary.

Configure the G700 and upgrade firmware

For a new installation of a G700 Media Gateway, you must complete the following configuration tasks:

Note:

The Avaya Gateway Installation Wizard (GIW) performs these tasks automatically.

- Assigning the IP addresses of the G700 media gateway components
 - Assigning the IP address for the P330 Stack Processor
 - Establishing IP routing for the stack
 - Assigning the IP address to the G700 media gateway processor
 - Assigning the default IP route to the G700 media gateway
 - Assigning IP addresses to the VoIP resources
 - Checking for IP connections
- Setting up the media gateway controller list
- Setting the LSP Transition Points

The Avaya Gateway Installation Wizard (GIW) can also perform the installation of new firmware on the G700 and media modules automatically. You identify the specific firmware filenames and the IP address of the TFTP server. The GIW then performs the following procedures:

- Installing new firmware on the P330 Stack Processor
- Installing new firmware on the G700 Media Gateway Processor
- Installing new firmware on the media modules

However, the GIW does *not* configure an X330 Expansion module. This task you must perform manually, as described in:

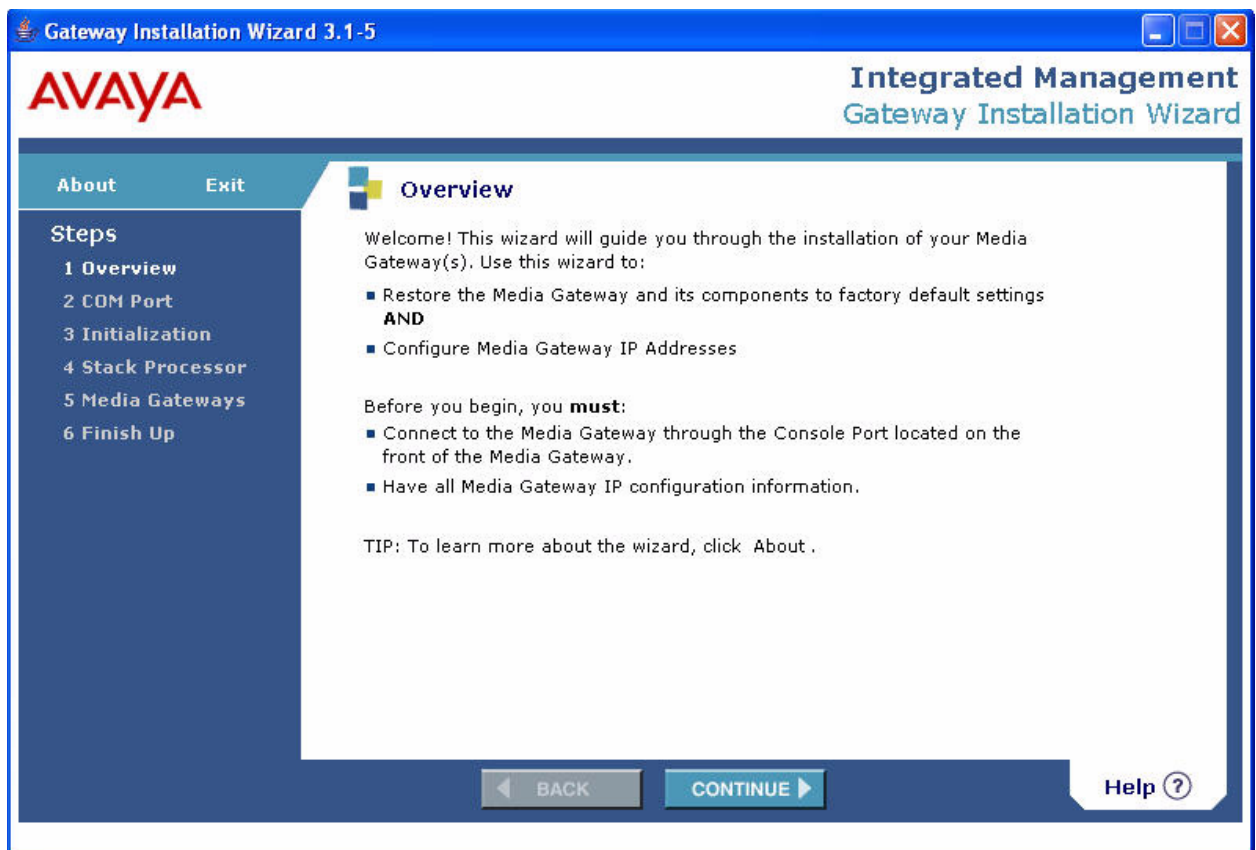
- [Configure an X330 Expansion Module \(If Necessary\)](#)

Connecting to the G700 console port

1. Plug one end of the provided flat RJ-45 to RJ-45 cable into the provided DB-9 adapter. See [Summary of S8300 and G700 Access Methods and Tasks](#) on page 42.
2. Plug the RJ-45 connector at the other end of the cable into the CON port of the G250.
3. Plug the DB-9 end of the flat cable into the COM port of the laptop computer.

4. From your laptop computer, double-click the GIW icon to run GIW.

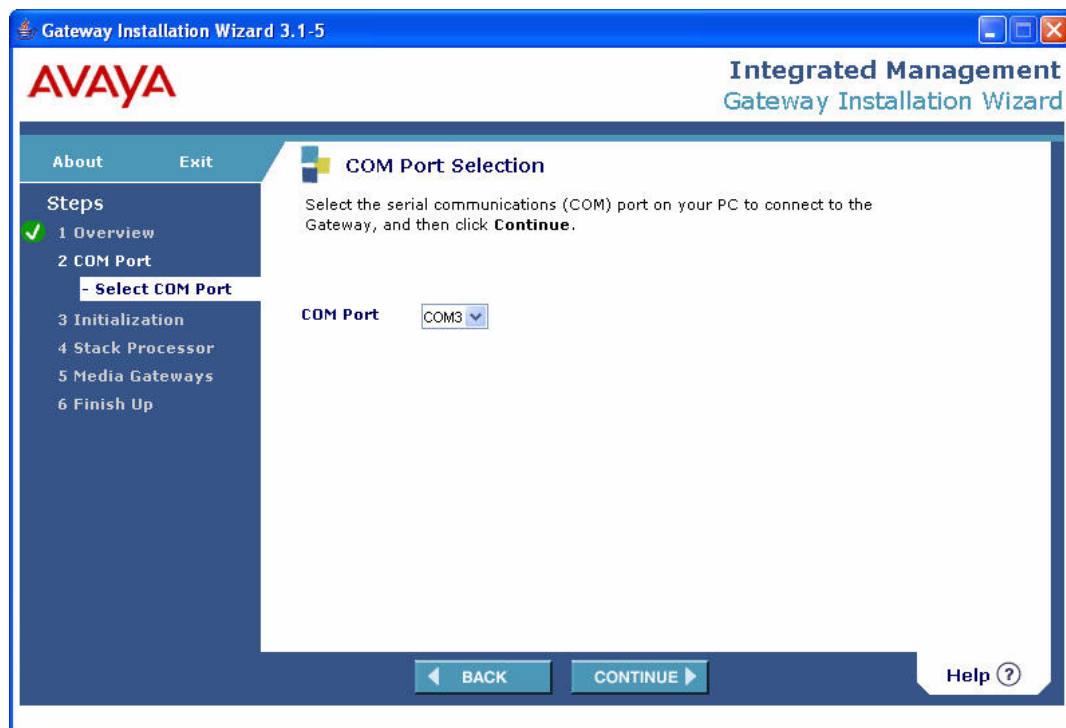
The Overview screen appears.



Installing a new G700 without an S8300 using the Gateway Installation Wizard

5. Click **Continue**.

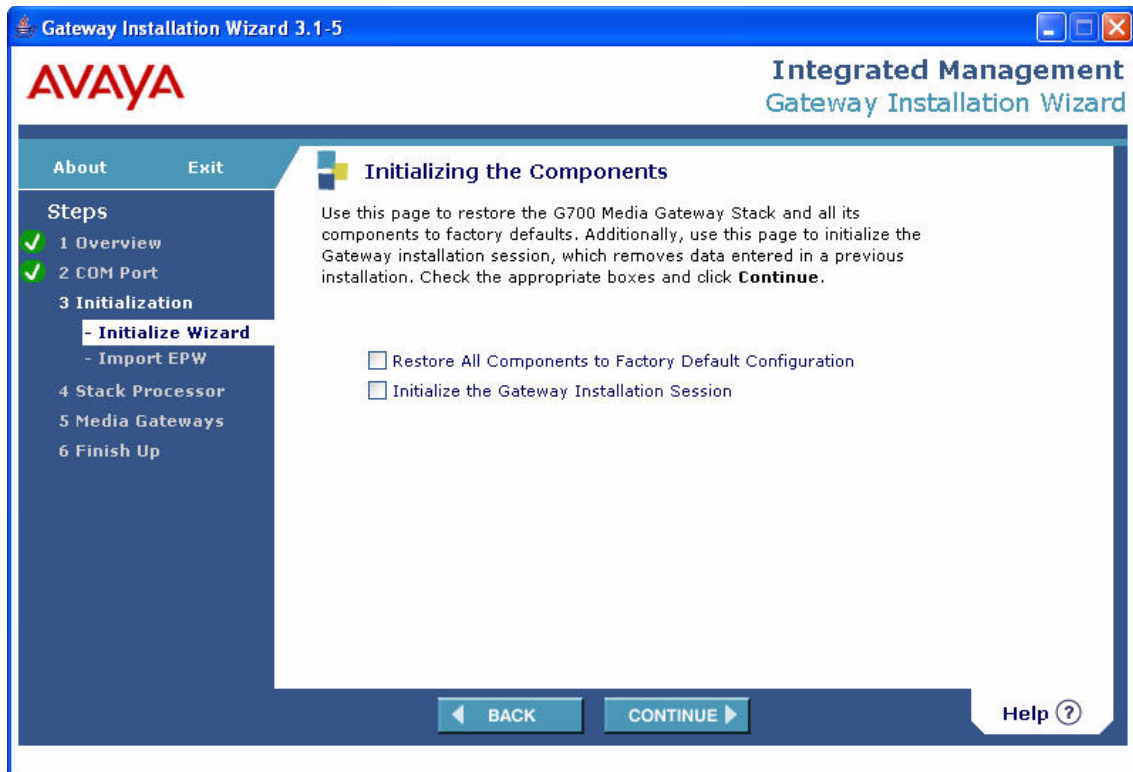
The COM Port Selection screen appears.



6. Select the COM port on the laptop that you are using to connect to the G250.

7. Click **Continue**.

The Initializing the Components screen appears.

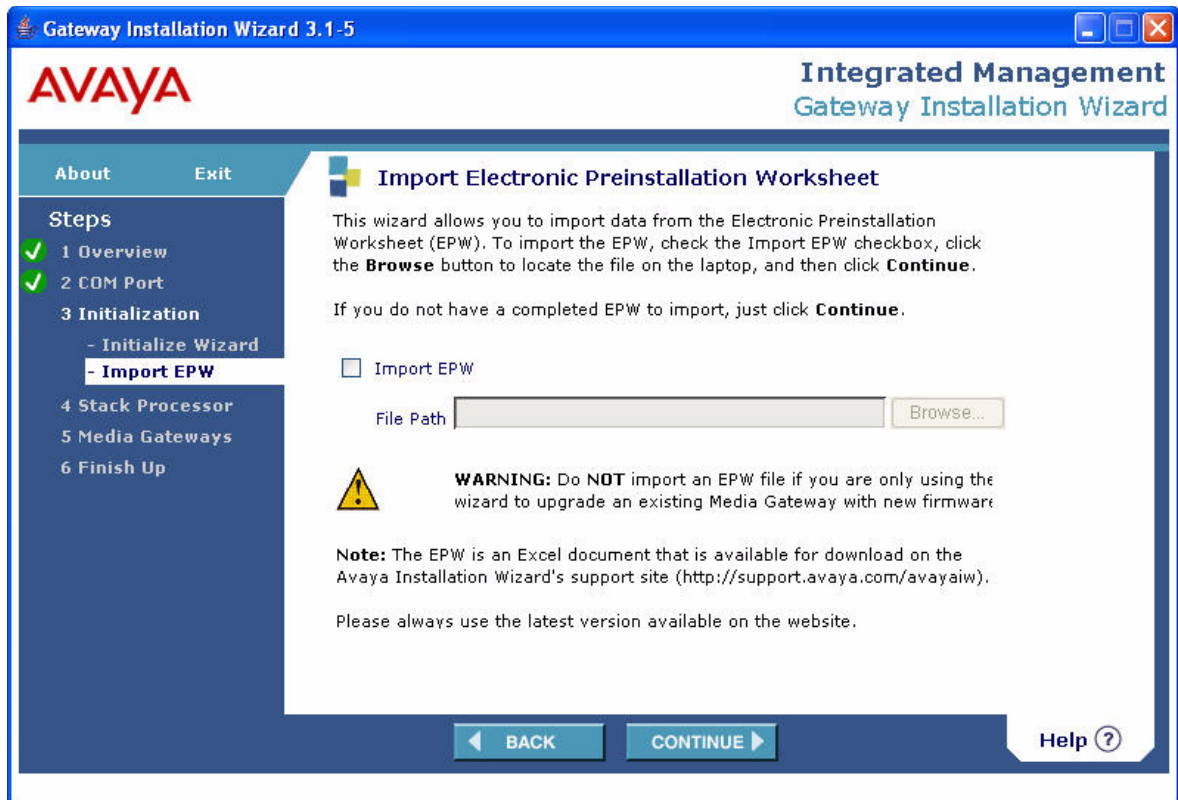


8. Select the **Restore All Components to Factory Default Configuration** and **Initialize the Gateway Installation Session** fields.

Installing a new G700 without an S8300 using the Gateway Installation Wizard

9. Click **Continue**.

The Import Electronic Preinstallation Worksheet screen appears.



10. If you are using an EPW to configure the G700 Media Gateway, do the following:

Note:

If you are using GIW to upgrade files or you do not have an EPW, do not check **Import EPW**.

- Check **Import EPW**.
- Click the Browse button, and locate and select the EPW file on your laptop.

Any values that are included in the EPW will appear as default values from now on as you move through this wizard.

11. Click **Continue**.

The P330 Stack Processor — IP Addresses screen appears.

Gateway Installation Wizard 3.1-5

AVAYA Integrated Management Gateway Installation Wizard

About Exit

Steps

- ✓ 1 Overview
- ✓ 2 COM Port
- ✓ 3 Initialization
- 4 Stack Processor
 - IP Addresses**
- 5 Media Gateways
- 6 Finish Up

P330 Stack Processor - IP Addresses

Configure the P330 stack processor to access the LAN. Type the required information, and then click **Continue**.

P330 Stack Processor

IP Address

Subnet Mask

VLAN Number

IP Routes	Destination IP Address	Network Gateway IP Address
1	0.0.0.0	1.2.3.254
2		(Optional)
3		(Optional)
4		(Optional)
5		(Optional)

◀ BACK CONTINUE ▶ Help ?

12. Complete the following fields for the P330 Stack Processor:

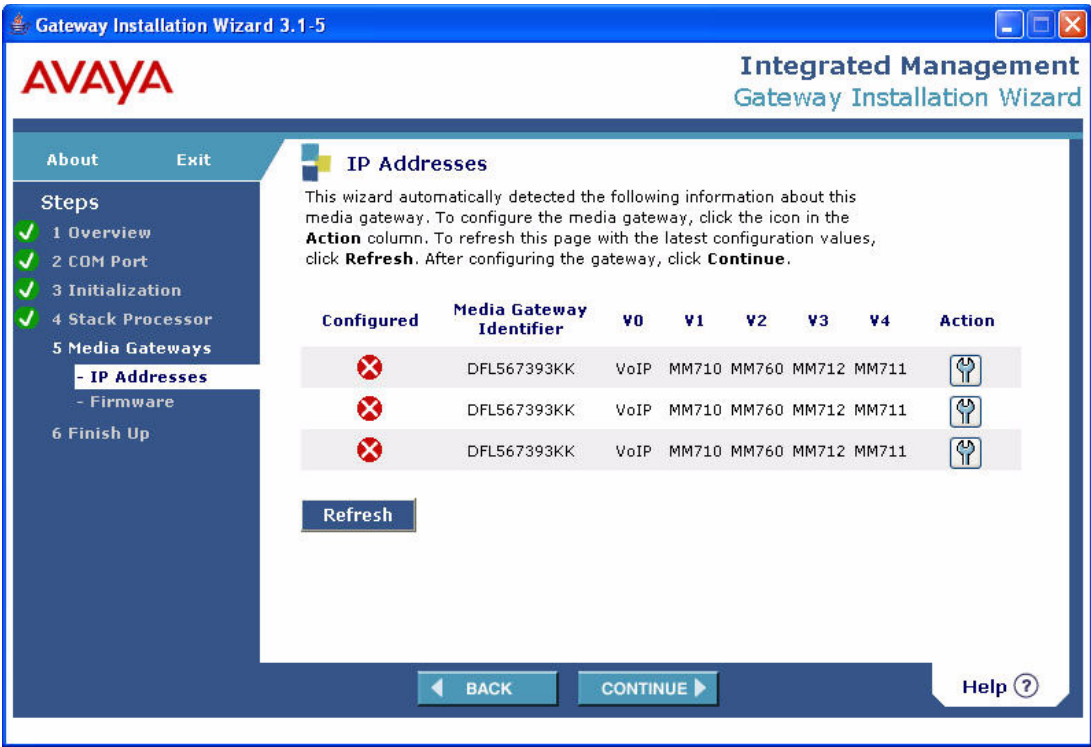
- **IP Address** — the IP address assigned to the P330 Stack Processor
- **Subnet Mask** — the subnet mask assigned to the P330 Stack Processor
- **VLAN Number** — the VLAN assigned to the P330 Stack Processor, normally the same VLAN assigned to the primary controller

13. In the **Destination IP Address** in the first **IP Routes** field, type 0.0.0.0.14. In the Network Gateway IP Address in the first **IP Routes** field, type the IP address of the customer's default network gateway.

Installing a new G700 without an S8300 using the Gateway Installation Wizard

15. Click **Continue**.

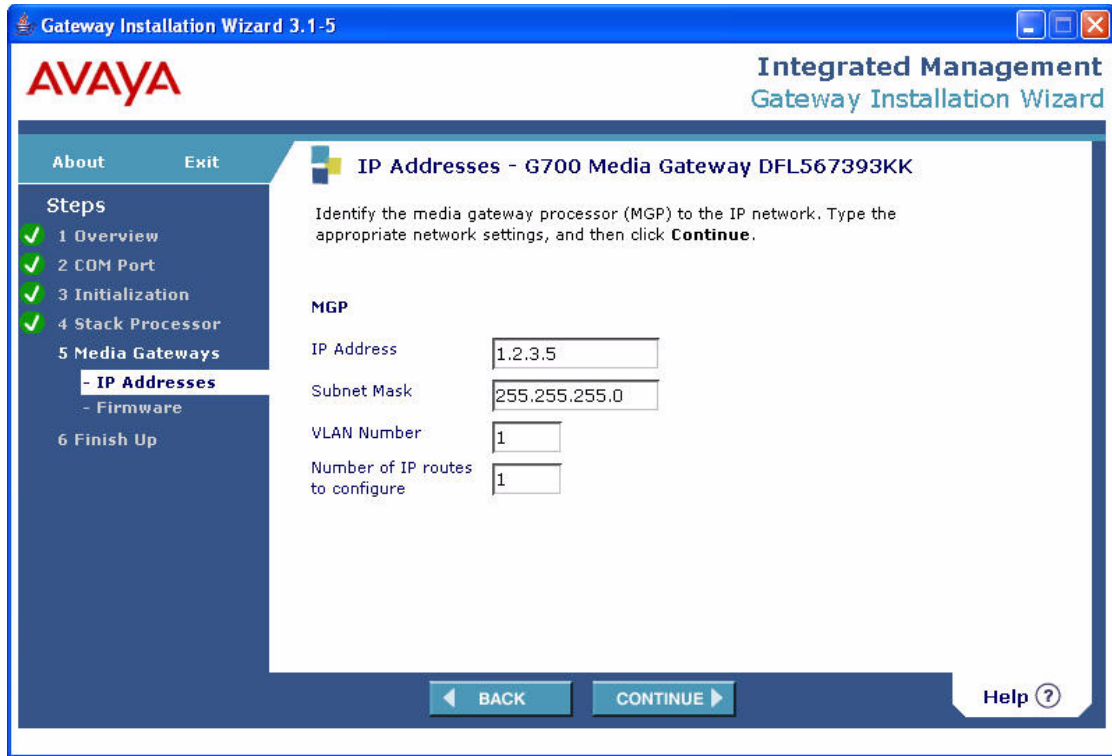
The IP addresses screen appears.



The IP Addresses screen displays information about the G700 automatically detected, such as what media modules are installed in the media modules slots.

16. Click the  icon in the Action column.

The IP Addresses — G700 Media Gateway screen appears.



Gateway Installation Wizard 3.1-5

AVAYA Integrated Management Gateway Installation Wizard

About Exit

Steps

- 1 Overview
- 2 COM Port
- 3 Initialization
- 4 Stack Processor
- 5 Media Gateways
 - IP Addresses
 - Firmware
- 6 Finish Up

IP Addresses - G700 Media Gateway DFL567393KK

Identify the media gateway processor (MGP) to the IP network. Type the appropriate network settings, and then click **Continue**.

MGP

IP Address

Subnet Mask

VLAN Number

Number of IP routes to configure

BACK CONTINUE

Help ?

17. Complete the following fields:

- **IP Address** — the IP address assigned to the Media Gateway Processor
- **Subnet Mask** — the subnet mask assigned to the Media Gateway Processor
- **VLAN Number** — the VLAN assigned to the Media Gateway Processor, normally the same VLAN assigned to the primary controller
- **Number of IP Routes** — the number of IP routes you are assigning to the Media Gateway Processor. The next screen allows you to define each IP route.

18. Click **Continue**.

The IP Route Addresses - G700 Media Gateway screen appears.

Gateway Installation Wizard 3.1-5

AVAYA Integrated Management Gateway Installation Wizard

About Exit

Steps

- 1 Overview
- 2 COM Port
- 3 Initialization
- 4 Stack Processor
- 5 Media Gateways
 - IP Addresses
 - Firmware
- 6 Finish Up

IP Addresses - G700 Media Gateway DFL567393KK

Identify the routing information for the MGP. Type the appropriate network settings, and then click **Continue**.

MGP

IP Routes	Destination IP Address	Destination Subnet Mask	Gateway IP Address
1	0.0.0.0	0.0.0.0	1.2.3.254

BACK CONTINUE

Help ?

19. Complete the fields as follows for each IP Route number:

- **Destination IP Address** — the default 0.0.0.0 or the IP address of the destination IP route
- **Destination Subnet Mask** — the default 0.0.0.0 or the subnet mask of the destination IP route
- **Gateway IP Address** — the IP address of the default network gateway for the route



CAUTION:

The default gateway IP routing address is required for Communication Manager 4.0.

20. Click **Continue**.

The Media Gateway Controller List screen appears.

Gateway Installation Wizard 3.1-5

AVAYA Integrated Management Gateway Installation Wizard

About Exit

Steps

- ✓ 1 Overview
- ✓ 2 COM Port
- ✓ 3 Initialization
- ✓ 4 Stack Processor
- 5 Media Gateways
 - IP Addresses
 - Firmware
- 6 Finish Up

IP Addresses - Media Gateway Controller List

Configure the media gateway controller list with the media servers that will provide call processing service for the media gateway. Additionally, configure the associated transition points used by the media gateway when searching for an alternate call processing controller in the case that the current call processing controller cannot be reached. Enter the required information and then click **Continue**.

Controller	Ping	IP Address
1		1.2.3.6
2		(Optional)
3		(Optional)
4		(Optional)

Ping Test

BACK CONTINUE

Help ?

21. Complete the **IP Address** field for each Controller number according to the following guidelines:

- The first IP address can be one of the following IP addresses:
 - For an S8700-series primary controller, the IP address of a C-LAN board that is connected to the primary controller.
 - For an S8400 or S8500 primary controller, the IP address of either a C-LAN board that is connected to the primary controller, or an Ethernet port, on the server itself, that has been enabled for processor Ethernet connections.
 - For an S8300 primary controller, the IP address of the S8300.
- The next three IP address parameters are optional IP addresses of up to three alternate controllers. Each of the three optional controllers can be a second C-LAN connected to the primary controller (S8400, S8500, or S8700-series Media Servers), an S8300 configured as an LSP, or the port enabled as the Ethernet processor port on an S8500 configured as an LSP. The types of alternate controllers in the list depend on the G700's primary controller and the other controller devices it supports.

Installing a new G700 without an S8300 using the Gateway Installation Wizard

22. Click **Continue**.

The VoIP Module IP Address screen appears.

Gateway Installation Wizard 3.1-5

AVAYA Integrated Management Gateway Installation Wizard

About Exit

Steps

- 1 Overview
- 2 COM Port
- 3 Initialization
- 4 Stack Processor
- 5 Media Gateways
 - IP Addresses
 - Firmware
- 6 Finish Up

IP Addresses - G700 Media Gateway DFL567393KK

Identify the IP addresses for all VoIP engines. Type the appropriate network settings, and then click **Continue**.

Voip Modules

Location	IP Address
V0	1.2.3.7
V2	

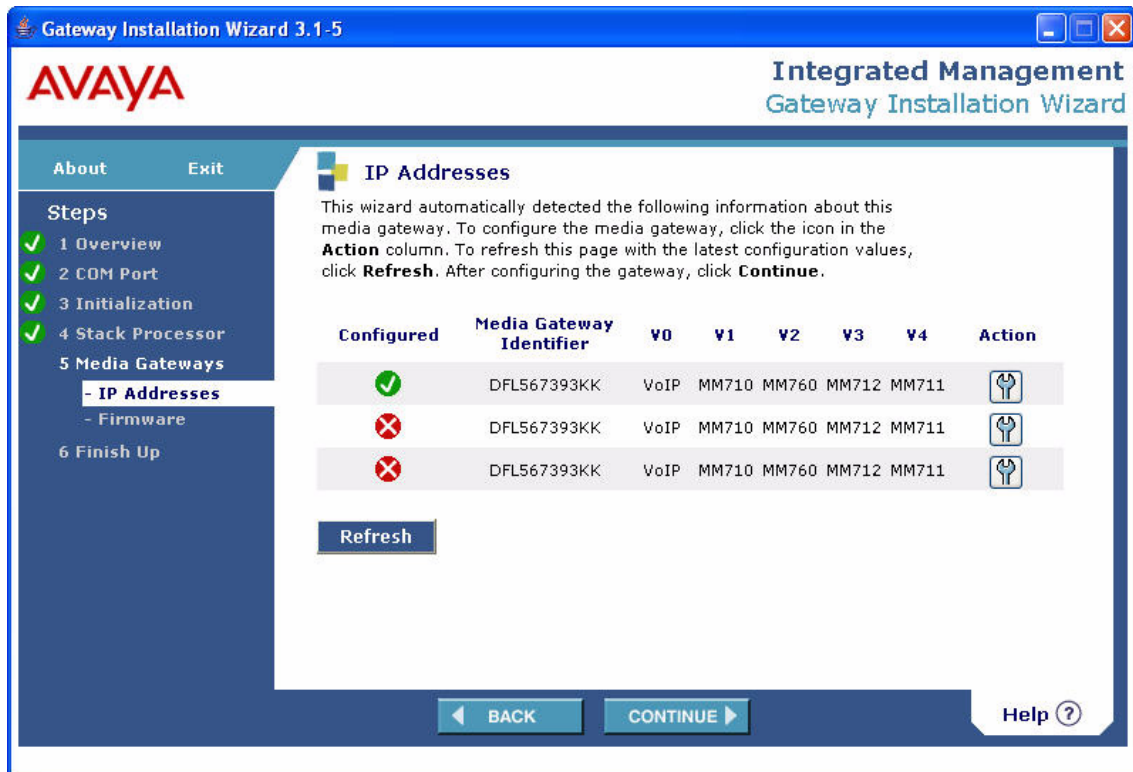
BACK CONTINUE

Help ?

23. For each VoIP Module Location, enter the IP address of the VoIP resource. **v0** designates the VoIP resource resident on the G700 Media Gateway motherboard. The MM760 VoIP Media Modules are designated according the slot (for example, **v1**, **v2**, **v3**, **v4**) in which the media module has been installed.

24. Click **Continue**.

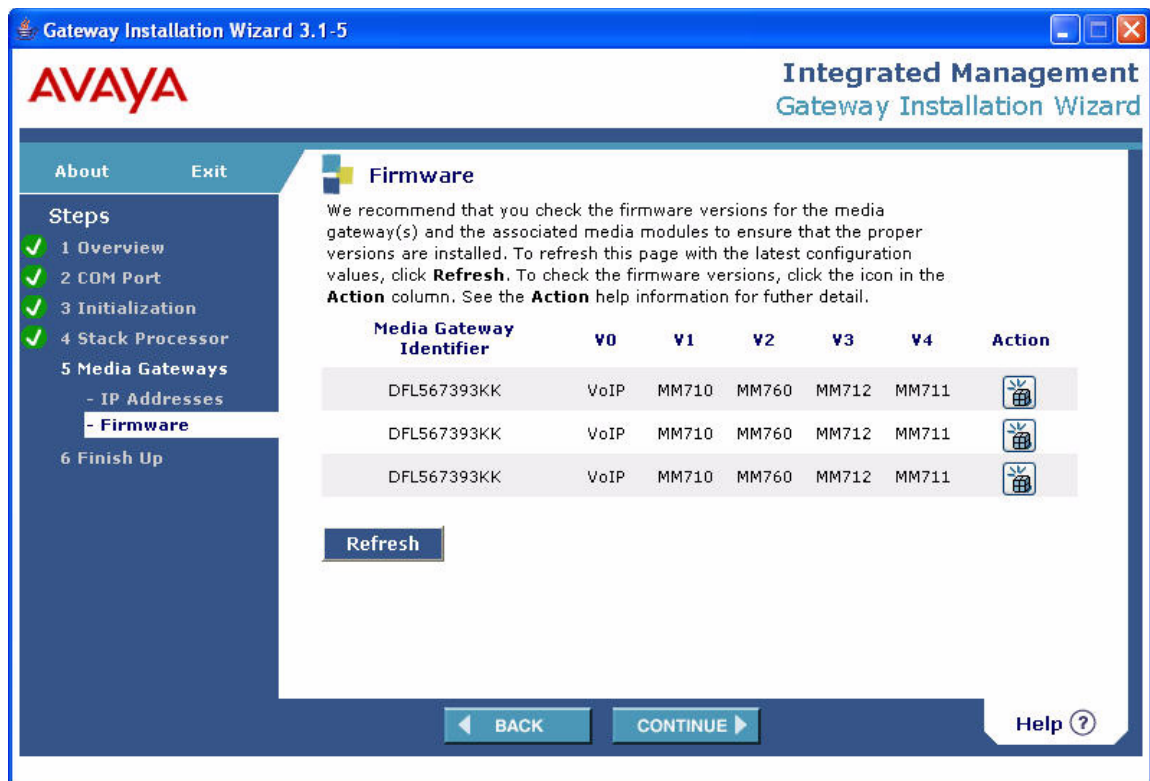
The IP Addresses screen reappears. In the **Configured** column, green checkmarks (✓) now appear to indicate a component has been configured.



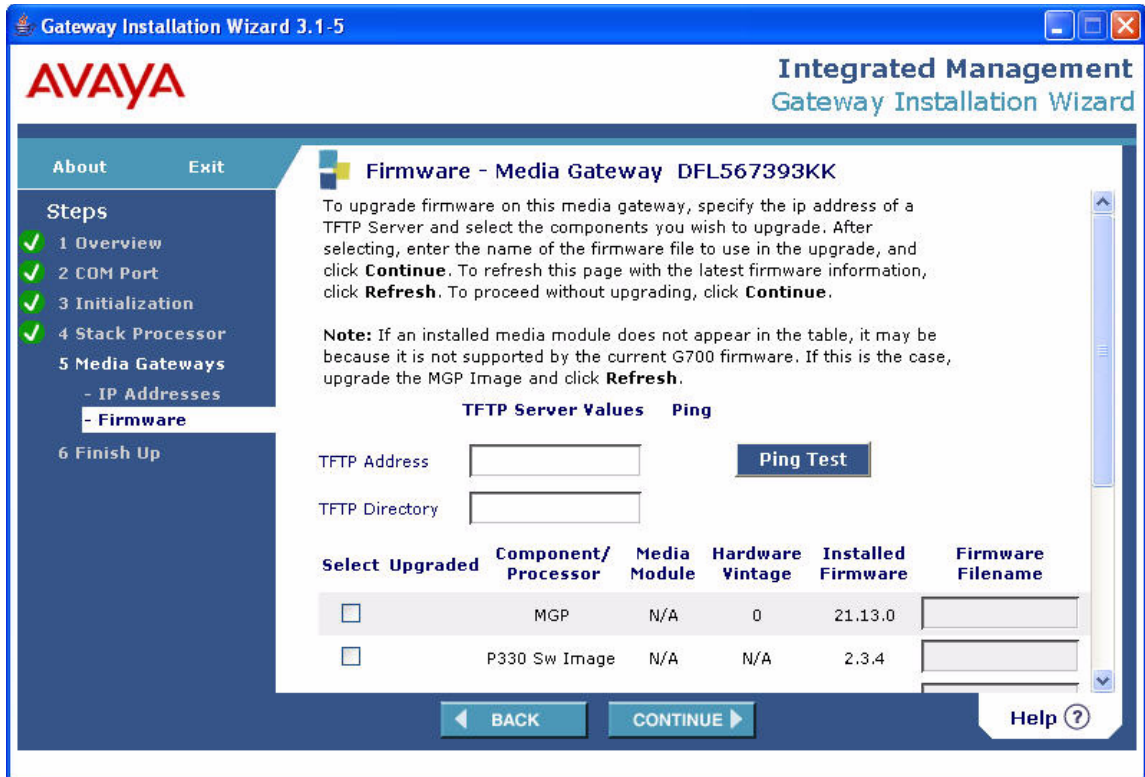
Installing a new G700 without an S8300 using the Gateway Installation Wizard

25. Click **Continue**.

The Firmware screen appears.



26. Click the firmware download icon  to update firmware on any of the G700 components.
The Firmware - Media Gateway screen appears.



The screenshot shows the 'Firmware - Media Gateway' screen of the Gateway Installation Wizard. The left sidebar lists steps: 1 Overview, 2 COM Port, 3 Initialization, 4 Stack Processor, 5 Media Gateways (selected), and 6 Finish Up. Under '5 Media Gateways', 'IP Addresses' and 'Firmware' are listed. The main area is titled 'Firmware - Media Gateway DFL567393KK'. It contains instructions on how to upgrade firmware, a 'Note' about unsupported modules, and a 'TFTP Server Values' section with input fields for 'TFTP Address' and 'TFTP Directory', and a 'Ping Test' button. Below this is a table with columns: 'Select Upgraded', 'Component/Processor', 'Media Module', 'Hardware Vintage', 'Installed Firmware', and 'Firmware Filename'. The table has two rows: one for 'MGP' and one for 'P330 Sw Image'. At the bottom are 'BACK' and 'CONTINUE' buttons, and a 'Help' link.

Steps

- 1 Overview
- 2 COM Port
- 3 Initialization
- 4 Stack Processor
- 5 Media Gateways
 - IP Addresses
 - Firmware
- 6 Finish Up

Firmware - Media Gateway DFL567393KK

To upgrade firmware on this media gateway, specify the ip address of a TFTP Server and select the components you wish to upgrade. After selecting, enter the name of the firmware file to use in the upgrade, and click **Continue**. To refresh this page with the latest firmware information, click **Refresh**. To proceed without upgrading, click **Continue**.

Note: If an installed media module does not appear in the table, it may be because it is not supported by the current G700 firmware. If this is the case, upgrade the MGP Image and click **Refresh**.

TFTP Server Values Ping

TFTP Address: Ping Test

TFTP Directory:

Select Upgraded	Component/Processor	Media Module	Hardware Vintage	Installed Firmware	Firmware Filename
☐	MGP	N/A	0	21.13.0	
☐	P330 Sw Image	N/A	N/A	2.3.4	

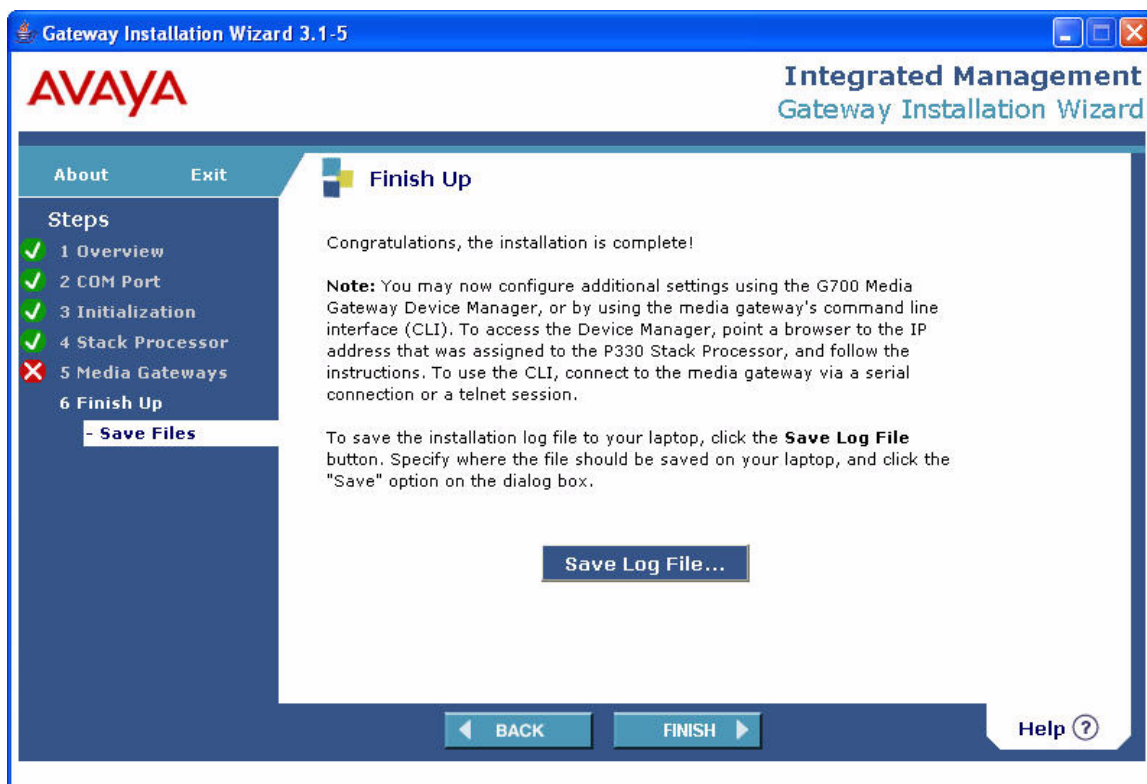
BACK CONTINUE Help ?

27. In the **TFTP Address** field, enter the IP address of the TFTP server on which the firmware resides.
28. In the **TFTP Directory** field, enter the directory path where the firmware files reside.
29. In the **Select Upgraded** column, select the components you want to upgrade.
30. In the **Firmware FileName** column, enter the firmware filename for each component you selected for upgrading.

31. Click **Continue**.

The Gateway Installation Wizard configures the G700 and its components and upgrades firmware you selected.

When the installation is complete, the Finish Up screen appears.



32. Click **Finish**.

Configure an X330 Expansion Module (If Necessary)

User Guides and Quick Start Guides for the expansion modules are available on the Avaya Support web site:

To configure an X330 Expansion Module

1. Go to the Avaya Support web site: <http://support.avaya.com>.
2. In the list on under Technical Database, click on **LAN, Backbone, and Edge Access Switches**.
3. Under Wiring Closet & Distribution, click on **P330 Stackable Switching System**.

4. Click on **All Documents**.
5. Select the appropriate document for the expansion module you are installing.

Set rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 Stack Processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 Stack Processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type `set spantree help` and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type `set spantree enable` and press **Enter**.
4. To set the **rapid spanning tree** version, type `set spantree version rapid-spanning-tree` and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command `set port spantree cost auto`.

Note:

Avaya P330 Stack Processors now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type `set port edge admin state module/port edgeport`.

For more information on the Spanning Tree CLI commands, see the *Avaya P330T User's Guide* (available at <http://www.avaya.com/support>).

Administer Communication Manager

Important:

The administration procedures in this section are done on the media server that is the primary controller for the new G700 you previously installed. This primary controller may or may not be the S8300 you installed in the G700.

The primary controller for the G700 you are installing must be administered to enable communication between the primary controller and the G700. The administration differs somewhat depending on whether the primary controller is an S8300 or the primary controller is an S8400, S8500, or S8700-series Media Server.

Perform one of the following two administration procedures in this section:

- [Administering an S8300 primary controller](#)
- [Administering an S8400, S8500, or S8700-series primary controller](#)

Administering an S8300 primary controller

CAUTION:

This administration applies only to the primary controller. If the S8300 you installed is configured as an LSP, do *not* perform this administration on it. Translations are automatically copied to the LSP from the S8300 primary controller.

Skip this section and go to [Administering an S8400, S8500, or S8700-series primary controller](#) on page 227 if the primary controller is an S8400, S8500, or S8700-series Media Server.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of administration required, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

2. Log in, and open a SAT session (type **sat** or **dsat**).
3. At the SAT prompt, type **reset system 4**
The system reboots.
4. After the reboot is complete, telnet to the S8300, login, and open a SAT session.

Assigning Node Names and IP Addresses for the LSPs

If the S8300 network configuration includes LSPs, they must be specified on the **Node Names** screen.

To assign node names

1. At the S8300 SAT prompt, type **change node-names ip** to open the **Node Names** screen.

Example Node Names Screen

change node-names ip		Page 1 of 1	
IP NODE NAMES			
Name	IP Address	Name	IP Address
default_____	0_.0_.0_.0_	_____	____.____.____.____
node-10-lsp	192.168.1_.50	_____	____.____.____.____
node-11-lsp	192.168.1_.51	_____	____.____.____.____
_____	____.____.____.____	_____	____.____.____.____
_____	____.____.____.____	_____	____.____.____.____
_____	____.____.____.____	_____	____.____.____.____

2. Enter the name and IP addresses for the LSPs.
3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 as primary controller, there will usually be one network region, defined as **1**. The procedure below uses **1** for the network region number as an example but the procedure applies for any network region number from **1** to **250**.

To define IP network region 1



CAUTION:

Defining IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see “*Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.”

1. At the SAT prompt, type **change ip-network-region 1**.

The S8300 displays the **IP Network Region** screen.

IP Network Region Screen

```
change ip-network-region 1                               Page 1 of 19
                                                         IP NETWORK REGION
Region: 1
Location:          Authoritative Domain:
Name:
MEDIA PARAMETERS                                     Intra-region IP-IP Direct Audio: yes
Codec Set: 1                                             Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                       IP Audio Hairpinning? y
UDP Port Max: 3048
DiffServ/TOS PARAMETERS                               RTCP Reporting Enabled? n
Call Control PHB Value: 34                             RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46                                   Use Default Server Parameters? y
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 7
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
AUDIO RESOURCE RESERVATION PARAMETERS
RSVP Enabled? n
```

2. If necessary, complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. Press **F3 (Enter)** to submit the screen.

Associating LSPs with Network Regions

If the primary controller has LSPs, you can associate each LSP with one or more network regions. In the event of a network failure, IP telephones assigned to a network region will register with an LSP associated with that region.

This procedure associates up to six LSPs with a network region.

To associate LSPs with a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be associated with region 1.
The LSP names must be the same as administered on the **Node Names** screen.
3. Submit the form.
4. Repeat for each network region with which you want to associate LSPs.

Administering IP Interfaces

This procedure assigns network region 1, as an example, to the S8300 media server.

To assign the network region and IP endpoint access to the S8300

1. At the SAT prompt, type **change ip-interfaces procr.**

The S8300 displays the **IP Interfaces** screen for the media server.

IP Interfaces Screen

```
change ip-interfaces procr                                     Page 1 of 1

                                IP INTERFACES

                                Type: PROCR

                                Node Name: procr
                                IP Address: 135.9.41.146
                                Subnet Mask: 255.255.255.0

                                Enable Ethernet Port? y
                                Network Region: 1
                                Allow H.323 Endpoints? y
                                Allow H.248 Gateways? y
                                Gatekeeper Priority: 5
```

2. The field **Enable Ethernet Port?** should indicate *y* (yes). The **Node Name** should be the IP address of the S8300 media server.
3. In the **Allow H.323 Endpoints** field, enter a 'y' to allow H.323 endpoint connectivity to the server.
4. In the **Allow H.248 Endpoints** field, enter a 'y' to allow H.248 media gateway connectivity to the server.
5. In the **Gatekeeper Priority** field, enter a value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to *y*.

Identifying LSPs to the S8300 primary controller

If the primary controller has LSPs, you must enter the LSP node names on the Survivable Processor form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the **LSP** screen, their status can be viewed with the **list survivable-processor** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **Survivable Processor** screen.

1. At the SAT command line, type **add survivable-processor <name>**, where *<name>* is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 19: Add Local Survivable Processor screen

add survivable-processor sv-mg2-lsp	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET	
Node Name: sv-mg2-lsp	
IP Address: 128.256.173.101	
Type: LSP	
Network Region: 1	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Skip to [Administering the Media Gateway](#) on page 237 to continue.

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

Complete the procedures in this section if the primary controller for the G700 you are installing is an S8400, S8500, or S8700-series Media Server. If the primary controller is an S8300, you should have completed the procedures in [Administering an S8300 primary controller](#) on page 222.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of required administration, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

For information on installing the CLAN boards on the S8400, S8500, or S8700-series port networks and complete information on installing an S8400, S8500, or S8700-series Media Server, see the Installation documentation on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

Assigning Node Names and IP Addresses for the C-LANs and LSPs

Note:

The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the S8400, S8500, or S8700-series Media Server. For information on how to upgrade the firmware, please see "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Media Servers and Gateways*, 03-300412.

To assign node names and IP addresses

1. At the SAT prompt, type `change node-names ip` to open the **Node Names** screen.

Example Node Names Screen

change node-names ipPage 1 of 1

IP NODE NAMES

Name	IP Address	Name	IP Address
default_____	0__ . 0__ . 0__ . 0__	_____	__ . __ . __ . __
node-1-clan_____	192.168.1__ . 124	_____	__ . __ . __ . __
node-2-clan_____	192.168.1__ . 97	_____	__ . __ . __ . __
node-10-lsp_____	192.168.1__ . 50	_____	__ . __ . __ . __
node-11-lsp_____	192.168.1__ . 51	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __

2. Enter the name and IP address for the C-LANs and LSPs.
3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 LSP and an S8500 or S8700-series Media Server as the primary controller, there may be more than one network region, since there can be up to 250 G700 media gateways connected to the S8500 or S8700-series Media Server with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700-series port networks, though they may also have the same network region.

Note:

With an S8300 or an S8400 Media Server, there still may be a need for more than one network region, though the S8400 supports up to five media gateways and the S8300 supports up to 50 media gateways.

The G700, in the case of multiple network regions, may also share the same network region as the CLAN board(s). However, it may have a different network region because of the geographic distances of the connections between the G700 and the primary controller. The G700 network region may also differ because of the nature of the endpoints connected to it.

To configure IP network regions for the G700 and CLAN board(s)



CAUTION:

Configuring IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

1. On the SAT screen of the primary controller for the G700 media gateway, type **change ip-network-region <network_region>**

where **<network_region>** is the region you will assign to the G700 media gateway. This region number may or may not match the network region of the S8400, S8500, or S8700-series CLAN boards.

The system displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain:		
Name:		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? y
UDP Port Max: 3048		
DiffServ/TOS PARAMETERS		RTCP Reporting Enabled? n
Call Control PHB Value: 34		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? y
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. Complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. If the network region of the G700 (1 in this example) is different from that of the S8400, S8500, or S8700-series CLAN board(s), you must interconnect the two regions.

Press **NextPage** twice to display page 3, of the **Inter Network Region Connection Management** screen.

This screen shows the source region (1) and the first 15 destination network region numbers. (Pages 4–19 show destination regions 16–250).

IP Network Region Screen, Page 3

display ip-network-region 1									
Inter Network Region Connection Management									
src	dst	codec	direct				Dynamic	CAC	
rgn	rgn	set	WAN	WAN-BW-limits	Intervening-regions		Gateway		IGAR
1	1	1							
1	2								
1	3								
1	4								
1	5								
1	6								
1	7								
1	8								
1	9	3							
1	10								
1	11								
1	12								
1	13								
1	14								
1	15								

4. Type the number for the type of codec set (1–7) that the S8400, S8500, or S8700-series Media Server will use to interconnect the G700 and the C-LAN board(s) in the row corresponding to the region of the C-LAN.

In this example, the C-LAN is in region 9 and codec-set type 3 is to be used for the interconnection between region 1 and region 9. (In this example, codec type 1 is used for communication within region 1)

The SAT command, **list ip-codec-set**, lists the types of codecs available on this server.

For more detail about the Inter Network Region Connection Management form, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

5. Press **F3 (Enter)** when complete.

Assigning LSPs to the Network Regions

If the primary controller has LSPs, you can assign the LSPs to network regions. In the event of a network failure, IP telephones assigned to a network region will register with the LSPs assigned to that region.

This procedure assigns up to six LSPs to a network region.

To assign LSPs to a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be assigned to region 1.
The LSP names must be the same as administered on the **Node Names** form.
3. Submit the form.
4. Repeat for each network region to which you want to assign LSPs.

Administering IP Interfaces

To define the IP interfaces of the S8400, S8500, or S8700-series port network CLAN boards

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type **change ip-interfaces <slot location>** to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces 01A03
Page 1 of 1

IP INTERFACES

Type: C-LAN
Slot: 01A03
Code/Suffix: TN799 d
Node Name: procr
IP Address: 135.9.41.146
Subnet Mask: 255.255.255.0
Gateway Address: 135.9.41.254
Enable Ethernet Port? y
Network Region: 1
VLAN: 0

Link: 1

Allow H.323 Endpoints? y
Allow H.248 Gateways? y
Gatekeeper Priority: 5

Target socket load:
Receive Buff TCP Window Size:

ETHERNET OPTIONS

Auto? n
Speed: 100 Mbps
Duplex: Full

2. Complete the fields as described the in [Table 11](#).

Table 11: IP interfaces field descriptions

Field	Conditions/Comments
Type	Either C-LAN.
Slot	The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799 for C-LAN.
Node name	The unique node name for the IP interface. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the C-LAN.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see “ <i>Administration for Network Connectivity for Avaya Communication Manager, 555-233-504</i> ”.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.

1 of 2

Table 11: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
VLAN	The VLAN number assigned to the C-LAN, if any.
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Receive Buffer TCP Window Size	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.
Link	This display only field shows the unique number for the Ethernet link. The Ethernet link was assigned on the data module form.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
Auto?	Enter 'y' or 'n' to set auto-negotiation.
Speed	Enter 10 or 100 Mbps if Auto was set to no.
Duplex	Enter half or full if Auto was set to no.

2 of 2

3. Close the screen.

To define the IP interface of the S8400 or S8500 processor Ethernet port

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type `change ip-interfaces procr` to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces procr		Page 1 of 1
IP INTERFACES		
Type: PROCR		
Node Name: procr		
IP Address: 135.9.41.146		
Subnet Mask: 255.255.255.0		Link: 1
Enable Ethernet Port? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
Target socket load:		

2. Complete the fields as described the in [Table 12](#).

Table 12: IP interfaces field descriptions

Field	Conditions/Comments
Type	Display only. PROCR
Node name	The unique node name for the IP interface. procr is the default node name. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the Processor Ethernet.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see <i>“Administration for Network Connectivity for Avaya Communication Manager, 555-233-504”</i> .
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.

1 of 2

Table 12: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
2 of 2	

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the LSP form, their status can be viewed with the **list survivable-processor** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

- At the SAT command line, type **add survivable-processor <name>**, where **<name>** is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 20: Add Local Survivable Processor screen

add survivable-processor sv-mg2-lsp	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET	
Node Name: sv-mg2-lsp	
IP Address: 128.256.173.101	
Type: LSP	
Network Region: 1	

4. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
5. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Administering the Media Gateway

To perform the procedures in this section, telnet to the primary controller, log in, and open a SAT session.



CAUTION:

Before administering a media gateway, make sure that the gateway has been fully configured.

In this section, you will do the procedures:

- [To add a media gateway](#)
- [To verify changes](#)
- [To enable announcements, if necessary](#)
- [To save Communication Manager translations](#)

To add a media gateway

1. At the SAT prompt, type `add media-gateway <number>`

where *<number>* is the gateway number from 1 to *n*. (*n* is 50 for an S8300, 5 for an S8400, and 250 for an S8500 or S8700-series Media Server).

The **Media Gateway** screen appears.

Add media gateway Screen

add media-gateway 1

Page 1 of 1

MEDIA GATEWAY

Number: 1Registered:
Type: g700FW Version/HW Vintage:
Name: SwainsonsIP Address:
Serial No: 012X06230551Controller IP Address:
Encrypt Link? yMAC Address: 00:04:0d:02:06:ca
Network Region: 1CF: 8 MB
Location: 1Site Data:
Recovery Rule: none

Slot	Module Type	Name
V1:		
V2:		
V3:		
V4:		
V9:		

2. Complete the **Name** field with the hostname assigned to the G700 media gateway.
3. Complete the **Identifier** field with the serial number of the G700 media gateway.

You can obtain the serial number by typing the **show system** command at the MGP command line interface.

CAUTION:

Be sure the serial number for the G700 media gateway you enter in this procedure matches *exactly* the serial number displayed in the **show system** command. The serial number is case-sensitive, and if entered incorrectly, will prevent the S8300 media server from communicating with the G700 media gateway.

4. Complete the **Network Region** field with the value supplied in the planning documentation.
5. If specifically requested by the customer or your planning documents, type **gateway-announcements** in the V9 field.

This field allows you to enable announcements on the G700 media gateway. V9 is a virtual slot. There is no announcement board associated with it. The announcements for the G700 are available in the G700 firmware and are administered in the same way as announcements on the TN2301 circuit pack used on S8400, S8500, or S8700-series port networks.

If there are multiple G700 media gateways sharing announcements, then enable announcements on the G700 whose trunks will receive the announcements most often.

6. Press **F3 (Enter)** to save your changes.

If properly administered, the G700 should register with the primary controller within 1–2 minutes. The **IP Address**, **MAC Address**, and **Module Type** fields are populated automatically after the G700 media gateway registers with the server.

7. Type **change media-gateway** to view the **Media Gateway** screen.

Media Gateway screen (after registration with primary controller)

```

change media-gateway 1                                     Page 1 of 1

                                MEDIA GATEWAY

      Number: 1                      Registered: y
      Type: g700                     FW Version/HW Vintage: 21.13.0 /0
      Name: Swainsons                 IP Address: 135.9.41.150
      Serial No: 012X06230551         Controller IP Address: 135.9.41.146
Encrypt Link? y                      MAC Address:
Network Region: 1                     CF: 8 MB
      Location: 1                     Site Data:
Recovery Rule: none

Slot  Module Type      Name
V1:   S8300            ICC MM
V2:   MM712            DCP MM
V3:   MM711            ANA MM
V4:   MM710            T1/E1 MM

V9:

```

The media modules installed in the G700 are listed next to their slot numbers. Verify that a G700 media gateway has been successfully added.

To verify changes

1. At the SAT prompt, type **list media-gateway**.

Media-Gateway Report screen

```

list media-gateway

                                MEDIA-GATEWAY REPORT

```

Number	Name	Serial No/ FW Ver/HW Vint	IP Address/ Cntrl IP Addr	Type	NetRgn RecRule	Reg?
1	LabA	01DR07128730 21 .13 .0 /0	135.177.49.57 135.177.49.59	g700	1 1	y
2	Data MG2	02DR01130356 11 .2 .0 /0	135.177.49.90 135.177.49.40	g350	1 none	n

2. Verify that the G700 media gateway has registered.

The `y` in the registered field signifies that the G700 media gateway has registered. If the G700 should become unregistered, the `y` will become an `n`, but the IP address will remain assigned to the G700 media gateway. If the G700 has never been registered, the IP Address field will be blank.

If the G700 fails to register, two common causes are:

- The serial number added as the **Identifier** for the G700 is wrong. To check, log back into the G700 gateway and type `show system`. Check the serial number that appears.
- There is no IP connection between the G700 and the S8300. To check, type `show mgc` and then `ping mgp <controller_address>`.

To enable announcements, if necessary

1. *Only if specifically requested by the customer or your planning documents*, at the SAT prompt, type `enable announcement-board <gateway_number> v9`

where `<gateway_number>` is the number of the G700 media gateway you added.

`v9` is the virtual slot (for example, `2v9` means media gateway number 2, slot V9).

2. Press **Enter** to enable announcements.

The system displays the message

Command successfully completed

To save Communication Manager translations

Save translations again after all Communication Manager administration is complete.

1. At the SAT prompt, type `save translation`

Complete the Installation Process

Consult the planning documentation to obtain the necessary information to complete the installation. Part of the final process will be to:

- Connect and administer test endpoints
- Test the endpoints
- Complete the electrical installation
- Enable adjunct systems

This completes the upgrade procedures.

Chapter 5: Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool

This chapter covers the procedures to upgrade the software on an installed Avaya S8300B or S8300C Media Server from a 2.x or 3.x release to 4.x. The procedures to upgrade the G700 firmware use CLI commands instead of the Upgrade Tool. This chapter also covers the procedures to upgrade the firmware on an installed Avaya G700 Media Gateway.



Important:

This chapter assumes that the currently installed S8300 is version B or C. The S8300B is required to run Communication Manager release 2.0 or greater. The S8300C is required to run Communication Manager release 4.0. If the currently installed S8300 is version A, follow the upgrade procedures in [Chapter 10: Manual upgrade of an S8300A and G700 to R4.0](#)



Important:

These procedures assume that you are upgrading an S8300 primary controller and/or any remote LSPs connected to the primary controller. If you are upgrading an LSP by itself locally, you cannot use the Upgrade Tool. Instead, you must follow the procedures in [Chapter 11: Manual upgrade of an existing S8300B or S8300C and G700 to R4.0](#).



Important:

If you are replacing the S8300B with an S8300C, use the procedures in [Chapter 12: Manual upgrade of an existing S8300B and G700 to S8300C with R4.0](#) on page 685.

Considerations for upgrading the S8300B as a primary controller or as an LSP

The S8300 can be configured as either the primary controller or as a local survivable processor (LSP). When the S8300 is an LSP, the primary controller, running Avaya Communication Manager, can be either another S8300 or an S8400, S8500, or S8700-series Media Server. These procedures assume the primary controller is an S8300.



CAUTION:

When you are upgrading the media server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the media server to a release that is not supported as an upgrade path, you might corrupt the translations.

Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.

To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access <http://support.avaya.com>. Select **Downloads > Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates > Latest Communication Manager Software & Firmware Compatibility Matrix**.

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

- The version of Communication Manager running on the LSP must be exactly the same as, or a later version that is compatible to, the version running on the primary controller.
- If upgrading both the primary controller and the LSP to the same release, you must upgrade the LSP first.
- The G700 Media Gateways should be upgraded after any LSPs and before the primary controller is upgraded.
- The Upgrade Tool is not available on an S8300 configured as an LSP. The Upgrade Tool is available only on the primary controller, so you use the Upgrade Tool on the primary controller to upgrade LSPs.



CAUTION:

This upgrade procedure requires a service interruption of approximately 2 hours, or up to 4 hours if IA770 is being used.

Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323



CAUTION:

Communication Manager Release 4.0 does not support the CWY1 integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current IA770 integration administration before the upgrade and then administer the integration to H.323 after the upgrade.

For instructions on converting the integration to H.323, including the removal of existing administration, see *Administering Media Servers to work with IA770*, 07-600788.



CAUTION:

Be sure to test the new integration before completing the upgrade.

The need to restore IP Phone files

If, before the upgrade, the existing system was serving as an http or tftp server for 4600-series IP Phone firmware downloads and configuration updates, the downloadable 4600-series IP Phone firmware and configuration file are *not* available on the server after the upgrade.

As a result, you must retrieve the 46xx firmware (the 46xx .tar file, for example **46xxH323_cm2_2_wi1_15_ipt2_2_111405.tar**) from the Avaya Downloads Web site and download the 46xx firmware file to the server after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the /tftpboot directory *after* the upgrade.

See the following:

- [Saving a copy of the 4600-series phone configuration file, if any](#) on page 264
- [Copying IP Phone firmware to the media server, if necessary](#) on page 297
- [Restoring the 4600-series phone configuration file, if any](#) on page 298

Major tasks to upgrade the S8300B to release 4.0 and upgrade the G700 firmware

The major tasks to upgrade the S8300B to release 4.0, and upgrade the G700 firmware are:

- [Before going to the customer site](#)
- [On-site Preparation for the Upgrade](#)

The Upgrade Tool performs the following tasks automatically:

- [Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways](#)
- [Post-upgrade tasks](#)

Before going to the customer site

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

This section covers:

- [Getting information that the project manager provides](#) on page 245
- [Getting the serial number of the G700, if necessary](#) on page 245
- [Checking the number of allocated ports](#) on page 245
- [Checking the versions of the LSPs \(if starting from R2.0 only\)](#) on page 246
- [Checking for and FTP/SCP/SFTP Server or Compact Flash for Backing up Data](#) on page 246
- [Obtaining S8300 software and G700 firmware](#) on page 246
- [Obtaining service pack files](#) on page 247
- [Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary](#) on page 249
- [Completing the RFA process \(obtaining license and password file\)](#) on page 250

Obtaining a USB DVD/CD-ROM drive

Upgrading Communication Manager on an S8300 to release 4.0 requires remastering the S8300B/C hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD/CD-ROM drive at the site.

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Getting the serial number of the G700, if necessary

For an upgrade of an existing G700, the existing license file can usually be reused. However, if the customer is adding feature functionality (for example, adding BRI trunks), or if the upgrade is between major releases (for example, 2.2 to 4.0), you will need the serial number of the G700.

To get the serial number of the G700 Media Gateway, ask the customer's administrator to:

1. Log in to the S8300 Maintenance web pages.
2. Select **View License Status** or **License File** from the main menu to display the serial number.

Note:

The serial number should also be on a sticker on the back of the G700 chassis, but this number is occasionally incorrect.

Checking the number of allocated ports

Release 4.0 of Communication Manager supports a maximum of 900 ports if the S8300 is a primary controller. If the existing system has more than 900 ports allocated, then there may be a problem with the upgrade and you need to escalate.

To check the system for the maximum number of ports, ask the customer to:

1. Log in to the SAT screen.
2. At the SAT command, **display system-parameters customer-options**.
3. Verify that the **Maximum Ports:** field is 900 or less.

Checking the versions of the LSPs (if starting from R2.0 only)

If you are upgrading a Communication Manager R2.0 server, the S8300 Media Server may be a version A. In this case, the server hardware must be replaced with an S8300B server. Similarly, LSPs may require a server replacement. You can check the version of S8300 hardware on LSPs by running the SAT command on the primary controller, `list config media-gateway <media gateway #>`, where `<media gateway #>` is the number of the media gateway containing an LSP. If you do not know which media gateways have LSPs, you can run the SAT command, `list media-gateway`.

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

During the installation and upgrade procedures, you must back up the system data to an FTP, SCP, or SFTP server.

If you are backing up data over the LAN, you normally use an FTP/SCP/SFTP server on the customer's LAN. To do this, you will need information on how to get to the backup location:

- Login ID and password
- IP address
- Directory path on the FTP server

If necessary, check with your project manager or the customer for this information.



Important:

Before going to the customer site, make sure that you can use either a customer server for backups or a compact flash card.

Obtaining S8300 software and G700 firmware

The files containing the software for the S8300 and the G700 and media module firmware are on the Communication Manager Software Distribution CD-ROM that you take to the site. This CD is called the software CD because it contains software for all of the Linux servers.

Additional files that are needed:

- License file
- Authentication file
- Software service pack files (most recent version)
- Security update files

Checking the CD for the most recent files

The media module and media gateway firmware on the Communication Manager software distribution CD may not be the most recent. Therefore, check the firmware versions contained on the software CD to verify that you have the latest before installing the firmware using the LSP's TFTP server. You can do this by accessing the CD on your laptop and displaying the actual firmware filenames in the Releases\<release_number>\Gateways directory.

For example, the CD may contain a file mm760v60.fdl, but the most recent firmware available on the Avaya Web site is mm760v65.fdl. In this case, download the mm760v65.fdl file from the Web site for installation instead of installing the file from the CD. As another example, the CD may contain the mgp_25_23_0.bin media gateway file, and the Avaya Web site also contains mgp_25_23_0.bin. In this case, you could use the firmware from the CD because the versions of the files are the same.



CAUTION:

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Obtaining service pack files

Pre- and post-upgrade service packs may be needed for this upgrade. If the service pack files are not on your software CD, download the service pack files from the Avaya Support web site to your laptop.

Pre-upgrade service pack (starting from R2.x only)

This upgrade requires a pre-upgrade service pack. The service pack filename differs, depending on which software load the media server is on. See [Table 13: Pre-Upgrade service pack filenames for software release and load](#) for the software load associated with each release.



CAUTION:

If the customer's system has Release 2.x of Communication Manager but has a field load other than those listed in the table, do not use this section to upgrade Communication Manager to Release 4.0. You must escalate.

Table 13: Pre-Upgrade service pack filenames for software release and load

Software release of existing media server	Associated software load	Service pack filename
Release 2.0	R012x.00.0.219.0	00.0.219.0-xxxx.tar.gz
Release 2.0.1	R012x.00.1.221.1	00.1.221.1-xxxx.tar.gz
Release 2.1	R012x.01.0.411.7	01.0.411.7-xxxx.tar.gz
Release 2.1.1	R012x.01.1.414.1	01.1.414.1-xxxx.tar.gz
Release 2.2	R012x.02.0.111.4	02.0.111.4-xxxx.tar.gz
Release 2.2.1	R012x.02.1.118.1	02.1.118.1-xxxx.tar.gz

Post-upgrade service pack

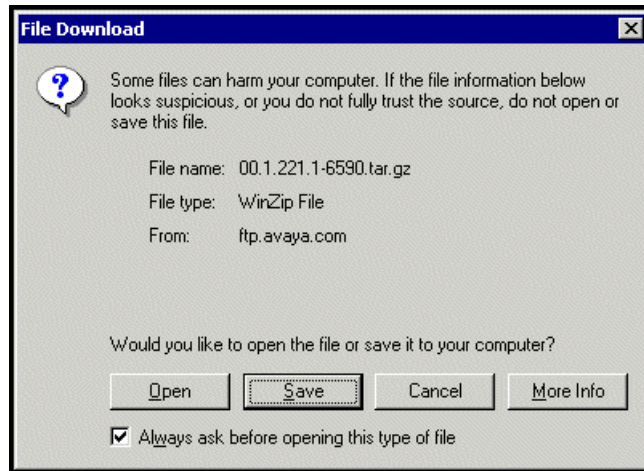
A post-upgrade service pack may be required. If so, download it from <http://www.avaya.com/support> on the Internet.

To download service packs to the laptop

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

The File Download window displays.

File download window



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

Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary

If IA700 is installed, determine whether a service pack is needed and/or optional languages are used. If so, you will need to obtain the data files.

Checking for IA770 stored messages size

When upgrading Communication Manager to release 4.0 from a previous release, the size of the messages stored in IA770 must be less than 72 hours due to a change in the voice encoding algorithm from CELP to G.711. Before the going to the site, have the customer check the size of messages stored in IA770 and, if greater than 72 hours, contact your service support center.

To check the IA770 stored messages size

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **System Configuration and Status > System Status**.

Look for "Used Hours of Speech" in the list. If more than 72 hours is reported, the customer must delete some messages before the upgrade.

Or, you can use the CLI command, `/vs/bin/util/vs_status`.

Obtaining an IA770 service pack file

If an IA770 service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an IA770 service pack file

1. On the Avaya Support website, double click on **Downloads**.
2. Under the heading **Download By Product Name**, select the letter **I** (for Intuity).
3. Select **IA 770 INTUITY AUDIX Messaging Application**.
4. Select **IA 770 INTUITY AUDIX Embedded Messaging Application Patches**.
5. Under Software Download, double click on the service pack for this release. For example, **IA 770 INTUITY AUDIX Embedded Messaging Application Patches for 1.3**.
6. Click on the file name appropriate for your release of Communication Manager software. For example, **C7022rf+a.rpm**
7. Click on **Save** and browse to the location on your laptop where you want to save the file.

Obtaining optional language files

Optional languages are any language other than English (**us-eng** or **us-tdd**). If optional languages will be used with this IA770, you can also download the appropriate language files from the Download Web site.

1. Follow the steps as in [Obtaining an IA770 service pack file](#) on page 250.
2. At step [4](#), select **IA 770 INTUITY AUDIX Embedded Messaging Application Languages**.

Completing the RFA process (obtaining license and password file)

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

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

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

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

Note:

For an upgrade, you do not normally need to install a new authentication file (with a .pwd extension). However, if one is required, follow the same steps as with a license file.

Downloading license file and password file for an LSP

The license file of the S8300 as a Local Survivable Processor must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300, S8400, S8500, or S8700-series Media Server). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

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

Note:

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

To download the license and password files to your laptop



Tip:

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

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and password files (for example, C:\licenses).
2. Access the Internet from your laptop and go to Remote Feature Activation web site, rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and password files for the customer.
4. Check that the license and password files are complete.
You might need to add the serial number of the customer's G700.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and password files to your laptop.

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

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

Note:

Business Partners call 800-295-0099. ART is available only to Avaya associates.

Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool

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

Note:

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

To run the ART

1. Access the ART web site on your laptop at <http://art.dr.avaya.com>.
2. Select **Administer S8x00 Server products for installation script**.
 - a. Log in.
 - b. Enter the customer information.
 - c. Select **Installation Script**.
 - d. Click **Start Installation script & IP Addr Admin**.

A script file is created and downloaded or emailed to you.

3. You can use the installation script to set up an IP address and other alarming parameters automatically.

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

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

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

Ensuring a super-user login exists

A super-user login must be administered prior to upgrading the system. The project manager, remote services, or the customer should check to verify that one exists. If a super-user login must be added, you must log in as *dadmin* or a higher level of login. You cannot add the login by logging in as *craft*.

Checking a pre-4.0 release

To ensure that a super-user login exists in Communication Manager prior to Release 4.0:

1. Log in with **telnet** or **ssh**.
2. At the SAT command line, enter **list logins**

The Logins screen appears.

```
list logins
```

Login	Service Level	Status	LOGINS				Expiration Date	No. of Sess. Sess. Used
			Pwd. Cycle	Aging (Days)	ASG	Blk		
init	init	active			y	n	/ /	
inads	inads	inactive			y	n	/ /	
dadmin	dadmin	inactive			n	n	/ /	
craft	craft	inactive			y	n	/ /	
acpsnmp	non-super-user	void			n	n	/ /	

3. Under the Service Level column, look for a login that has either the dadmin or super-user level.
4. If a super-user login does not exist, create one. See [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#) on page 254.

Checking a 4.0 release

To ensure that a super-user login exists in Communication Manager in Release 4.0 or higher:

1. Log in with **ssh**.
2. At the Linux command line, type **cat /etc/passwd | grep 555**.

The following list of super-user logins appears.

```
init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1001:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash
```

3. Look for any logins other than the init, inads, and craft logins. If no additional super-user logins exist, you must create one. See [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 255.

Creating a super-user login, if one does not exist (releases earlier than Release 4.0)

If a super-user login does not exist, one must be added before you can complete the upgrade. The customer or remote services should complete the following task.

1. Use the following steps only if you are starting from a software release *earlier* than Release 4.0:

Note:

Adding a super-user login with the SAT command line requires a dadmin, init, or inads login.

Note:

If you are upgrading an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

2. At the SAT command line, enter add login.

The Login Administration screen appears.

add loginPage 1 of x

LOGIN ADMINISTRATION

Password of Login Making Change:

LOGIN BEING ADMINISTERED

Login's Name:xxxxxxx

Login Type:

Service Level:

Disable Following a Security Violation?

Days to Disable After Inactivity:

Access to INADS Port?

LOGIN'S PASSWORD INFORMATION

Login's Password:

Reenter Login's Password:

Password Aging Cycle Length (Days):

LOGOFF NOTIFICATION

Facility Test Call Notification?

Acknowledgment Required?

Remote Access Notification?

Acknowledgment Required?

ACCESS SECURITY GATEWAY PARAMETERS

Access Security Gateway?

3. In the **Password of Login Making Change** field, type your password.

4. In the **Login's Name** field, type a login name agreed upon with the customer. Alternatively, a Business Partner may add the dadmin login.
5. In the **Login Type** field, type **customer**.
6. In the **Service Level** field, type **super-user**.
7. In the **Days to Disable After Inactivity** field, type **90**.
8. In the **Login's Password** field, type a password.
9. In **Reenter Login's Password** field, type the password again.
10. In the **Password Aging Cycle Length** field, type 90, and press **Enter**.
11. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.
 - a. Log in with `telnet` or `ssh`.
 - b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

Creating a super-user login, if necessary, for R4.0 or higher

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages. Use the following steps only if you are starting from Release 4.0 software or later:

Note:

A craft level login can create a super-user login in Release 4.0 or later.

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

To create a login:

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

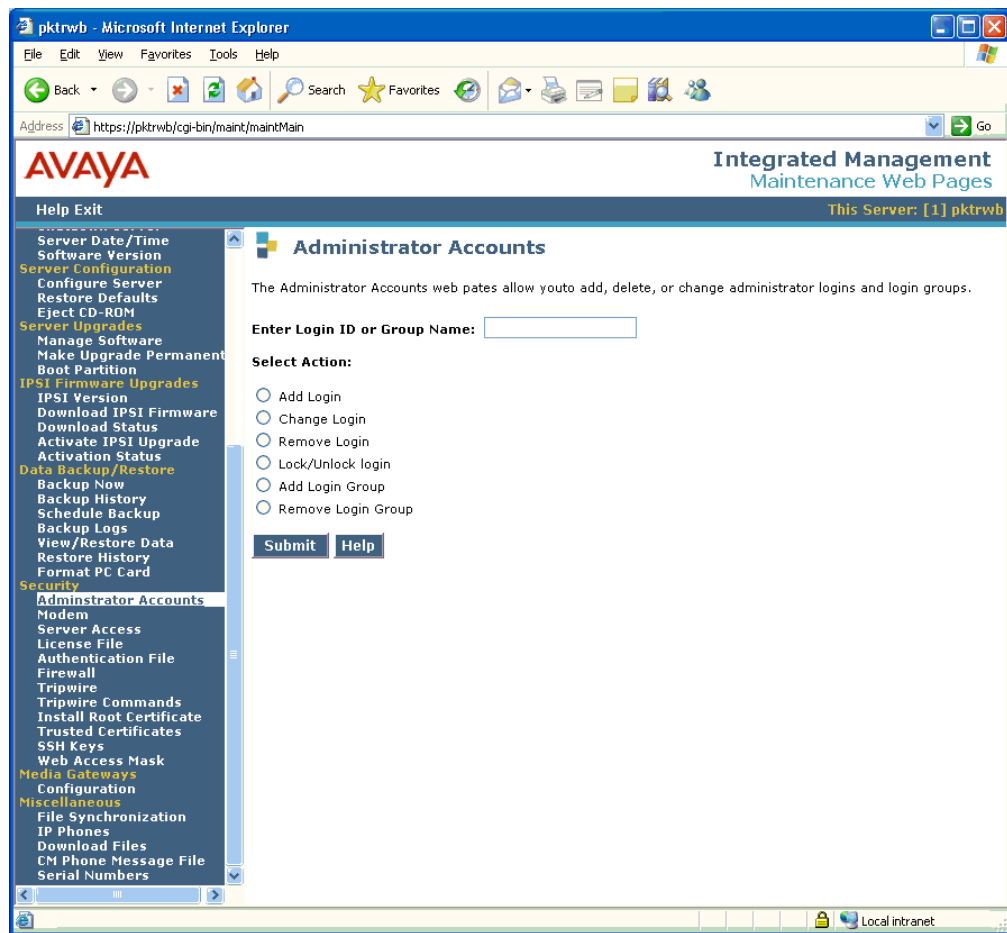
Note:

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

Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



3. Type the login name in the **Enter Login ID or Group Name** field.

4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The top navigation bar includes the Avaya logo, 'Help', 'Exit', and server information: 'This Server: [1] sv-gertrude1' and 'Duplicate Server: [2] sv-gertrude2'. A left sidebar contains a tree view of system management options, with 'Administrator Accounts' selected under the 'Security' section. The main content area is titled 'The Administrator Logins -- Add login web page allows you to add a new administrator login.' and contains the following form fields:

- Login ID:** Pre-filled with 'randy'.
- login group:** Text input field containing 'susers'.
- additional groups:** Text input field containing 'prof18'.
- allow Linux shell access:** A checkbox that is currently unchecked.
- lock this account:** A checkbox that is currently unchecked.
- date (YYYY-MM-DD) on which account is disabled (blank to ignore):** An empty text input field.
- select type of authentication:** Two radio button options: 'password' (selected) and 'ASG'.
- enter key or password:** A text input field.
- re-enter key or password:** A text input field.
- force password/key change on first login:** Two radio button options: 'yes' and 'no' (selected).
- maximum Number of days a password may be used (PASS_MAX_DAYS):** A text input field containing '90'.
- minimum number of days allowed between password changes (PASS_MIN_DAYS):** A text input field containing '90'.
- minimum acceptable password length (PASS_MIN_LEN):** A text input field containing '8'.
- number of days warning given before a password expires (PASS_WARN_AGE):** An empty text input field.
- days after password expires to lock account (0=immediate):** An empty text input field.

At the bottom of the form are 'Add' and 'Help' buttons. The browser's status bar at the very bottom shows 'Done' and 'Internet' connectivity.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

10. Complete the following fields:

- enter a challenge key or password
- re-enter challenge key or password
- force password/key change on first login

Note:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

- a. Log in with `telnet` or `ssh`.
- b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

On-site Preparation for the Upgrade

Perform the following tasks before starting the software upgrade on the S8300:

- [Setting up a TFTP server or HTTP server for LSP software download, if desired](#) on page 259
- [Accessing the S8300](#) on page 260
- [Removing the administration for the IA770 integration if CWY1 board is used](#) on page 260
- [Completing pre-upgrade tasks — If the target S8300 is the primary controller](#) on page 261
- [Saving a copy of the 4600-series phone configuration file, if any](#) on page 264
- [Getting IA770 \(AUDIX\) Data and Stopping IA770 \(if IA770 is being used\)](#) on page 265
- [Backing up S8300 recovery system files](#) on page 269
- [Copying the service pack files to the media server \(starting from R2.x only\)](#) on page 272
- [Installing the pre-upgrade software service pack \(starting from R2.x only\)](#) on page 272
- [Copying Files to the S8300 hard drive](#) on page 273
- [Copying authentication files to the LSPs](#) on page 275

- [Copying the Communication Manager software and media gateway firmware to a TFTP or HTTP server](#) on page 275
- [Copying the Communication Manager software and media gateway firmware to the server](#) on page 275
- [Preparing LSPs](#) on page 275

Setting up a TFTP server or HTTP server for LSP software download, if desired

The Communication Manager software CD-ROM can be used to load software on each LSP prior to running the upgrade, but this method requires the physical insertion of the CD-ROM into a CD-ROM drive attached to each LSP's S8300 server. Alternatively, the customer can set up one or more TFTP servers from which to download Communication Manager software to each LSP. However, the TFTP server or servers must be accessible to all LSPs over the WAN. Additionally, the file structure should be installed on the TFTP server so it matches the format of the CDROM. This means that, within the outgoing root directory of the TFTP server, a **/Releases** subdirectory must be established and all software or firmware should be copied to the TFTP server should be copied as subdirectories and files under the **/Releases** directory.

As another alternative, the customer can set up a Web server to be used to distribute the files. The file structure should be installed on the HTTP server so it matches the format of the Communication Manager software distribution CD. The source directory should be designated as URL of the web server followed by full path name to the **/Releases** directory. Example (<http://www.acme-home.com/upgrades/Releases>).

Note:

Use of the TFTP server should be within the local LAN segment. Downloading the Communication Manager software over a WAN is not recommended because a TFTP server can time out, and the download can fail.

Additionally, the bandwidth of the WAN should be large because the Communication Manager software files are very large ó with some files up to 72 Megabytes (MB) in size and a cumulative total for all files of over 400 MB.

Note:

To upgrade the firmware on the media gateway or its media modules, you can download the firmware from a TFTP server only. This TFTP server can be the **/tftpboot** directory on an S8300 Media Server or a TFTP directory on any server that is accessible over the LAN to the media gateway.

An HTTP server *cannot* be used for firmware downloads to the media gateway or its media modules.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See [Laptop configuration for direct connection to the services port](#) on page 42.

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

- [Accessing the server's command line interface with SSH](#) on page 55
- [Logging in to the media server from your laptop using Telnet](#) on page 56
- [Logging in to the S8300 Web Interface from your laptop](#) on page 57

Removing the administration for the IA770 integration if CWY1 board is used

Note:

If the S8300 is configured as an LSP, skip to [Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways](#) on page 281.



CAUTION:

Communication Manager Release 4.0 does not support the CWY1 method of integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current switch integration administration now. You will administer the integration for H.323 after the upgrade.

For instructions on removal of existing CWY1 administration, see *Administering Media Servers to work with IA770*.

Note:

For Releases 2.0 and 2.1 of Communication Manager that use IA770, you *cannot* remove messaging from the Media Gateway screen in the SAT interface *before* the upgrade. Therefore, you must remove messaging from Slot V8 of the Media Gateway screen after the upgrade, then administer the H.323 integration.

Completing pre-upgrade tasks — If the target S8300 is the primary controller

If the S8300 is configured as an LSP, skip to [Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways](#) on page 281.

**CAUTION:**

If you are upgrading an S8300 primary controller that has LSPs registered to it, the LSPs must be upgraded **before** the primary controller. (You can use the SAT command, `list media-gateway`, to see if there are LSPs registered to the S8300.)

Perform the following procedures if you are upgrading an S8300 that is configured as a primary controller:

- [To clear alarms](#)
- [To check link status](#)
- [To record all busyouts](#)
- [To disable scheduled maintenance](#)
- [To check for translation corruption](#)
- [To save translations](#)
- [To disable alarm origination](#)

Note:

It is no longer necessary to disable Terminal Translation Initialization (TTI) before an upgrade or to enable it after an upgrade.

To clear alarms

1. On the Maintenance Web Interface under Alarms, click **Current Alarms**.
2. If no alarms are listed, skip the next two steps.
3. If alarms are listed, click **Clear All**.
4. Resolve any remaining major alarms through the Communication Manager SAT.

To check link status

1. Open a SAT session.
2. Enter `display communication-interface links`.
Note all administered links.
3. Enter `status link number` for each administered link.
4. Enter `list signaling group`.
Note the signaling groups listed by number.
5. For each of the signaling groups listed, enter `status signaling group number`.
Make a note (write down) of any links that are down.

To record all busyouts

1. At the SAT prompt, type `display errors` and press **Enter**.
2. Look for type 18 errors and record (write down) any trunks that are busied out — you will return them to their busy-out state after the upgrade.

To disable scheduled maintenance

Scheduled daily maintenance must not interfere with the upgrade.

1. At the SAT prompt, type `change system-parameters maintenance` and press **Enter**.
2. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

or,

If scheduled maintenance is not in progress, set the **Start Time** field to a time after the upgrade will be completed.

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

To check for translation corruption

1. At the SAT prompt, type **newterm** and press **Enter**.
2. Enter your terminal type and press **Enter**.

If you see the message,

```
Warning: Translation corruption found
```

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To save translations

1. At the SAT prompt, type **save translation** and press **Enter**.
2. Under **Command Completion Status** you should see *Success*.

To disable alarm origination

If alarm origination is enabled during the upgrade, unnecessary alarms will be sent to the Operations Support System (OSS) destination number(s). Even if you selected **Suppress Alarm Origination** when you logged in, alarm origination will be automatically re-enabled when the system reboots after the software upgrade. Use this procedure to prevent alarm origination from being re-enabled after reboot.

**CAUTION:**

If you do not disable alarm origination, the system can generate alarms during the upgrade, resulting in unnecessary trouble tickets.

1. Logoff the SAT session.
2. At the command prompt, type **almenable -d n -s n**, where
 - d n sets the dialout option to **neither** (number)
 - s n disables SNMP alarm origination

Note:

Be sure to reset alarm origination after the upgrade.

3. Type **almenable** (without any options) to verify the alarm origination status.

You should see:

```
incoming: enable
```

```
Dial Out Alarm Origination: neither
```

```
SNMP Alarm Origination: n
```

Saving a copy of the 4600-series phone configuration file, if any

During an upgrade, any data in the `/tftpboot` directory is overwritten with new software and firmware. If the system was using the http or tftp capability for 4600-series phone firmware downloads and configuration updates, the firmware and 4600-series phone configuration file are overwritten.

You must redownload the 46xx firmware file after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the `/tftpboot` directory *after* the upgrade.

To copy the 4600-series configuration file to a safe location, perform the following steps:

1. Access the server's command line interface using telnet and an IP address of `192.11.13.6`.
2. Log in as `craft`.
3. At the Linux command line, type `cd /tftpboot`, and press **Enter**.
4. At the prompt, type `ls 46*`, and press **Enter**.

If a named **46xxsettings.txt** may appear in the list, or the prompt may reappear with no files listed. If the file name does not appear, there is no file to copy. You are finished with this procedure.

5. If the file name **46xxsettings.txt** appears, at the Linux command line, type `cp 46xxsettings.txt ~ftp/pub`.

The 4600-series phone settings file is now in a protected directory, `/var/home/ftp/pub`, and will not be overwritten during the upgrade. You will copy this file back to the `/tftpboot` directory after the upgrade.

Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used)

Skip to [Backing up S8300 recovery system files](#) on page 269 if IA770 is not being used.

If IA770 is being used, you need to collect optional language data (if this had not been done before arriving at the site), leave a test message, and shut down IA770 before backing up the files.

Determining whether optional languages are needed

To determine the system language

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Global Administration**; then **Messaging Administration**.
3. Enter the *craft* password.
4. At the command prompt, enter **display system-parameters features**.

The **SYSTEM PARAMETERS FEATURES** screen displays.

5. Go to page 3.

System Parameters Features screen

```

redtail           Active           Alarms: none           Logins: 1
display system-parameters features           Page 3 of 4
SYSTEM-PARAMETERS FEATURES

CALL TRANSFER OUT OF AUDIX
Transfer Type: enhanced_cover_0           Transfer Restriction: digits
Covering Extension: 50104

ANNOUNCEMENT SETS
System: us-eng           Administrative:

RESCHEDULING INCREMENTS FOR UNSUCCESSFUL MESSAGE DELIVERY
Incr 1: 0 days 0 hrs 5 mins           Incr 2: 0 days 0 hrs 15 mins
Incr 3: 0 days 0 hrs 30 mins           Incr 4: 0 days 1 hrs 0 mins
Incr 5: 0 days 2 hrs 0 mins           Incr 6: 0 days 6 hrs 0 mins
Incr 7: 1 days 0 hrs 0 mins           Incr 8: 2 days 0 hrs 0 mins
Incr 9: 7 days 0 hrs 0 mins           Incr10: 14 days 0 hrs 0 mins

enter command: display system-parameters features
Cancel Refresh Enter ClearFld Help Choices NextPage PrevPage

```

6. Under **Announcement Sets**, note the main system language listed after **System:** In this example, the main system language is English (**us-eng**). If the system language is anything other than **us-eng** or **us-tdd**, you will need to download the appropriate language files from a language CD after the upgrade.

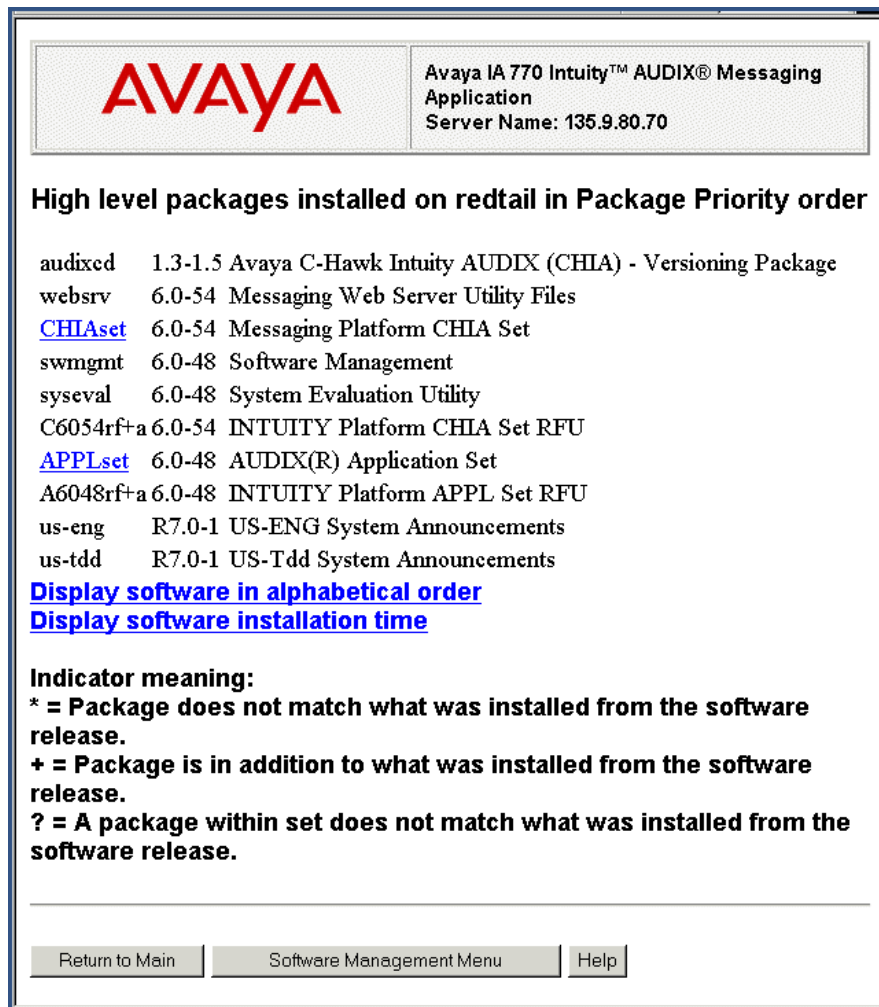
Note:

Starting with release 2.1, only English language files (**us-eng** and **us-tdd**) are included with the Communication Manager software. Before release 2.1, Latin American Spanish and Canadian French (**lat-span** and **french-c**) were also included.

To determine other languages

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Utilities**; then **Software Management**; then **Messaging System Software Display**.
The **Messaging System Software Display** screen displays.

Messaging System Software Display screen



3. Note the **System Announcement** language files listed. In this example, **us-eng** and **us-tdd** are listed. If any language files other than these two are listed, you will need to download the additional language files from a language CD after the upgrade.

Downloading optional language files, if needed

Skip to [To shut down IA770](#) on page 268 if optional language files are not needed. If the optional language files are needed, copy the files from the language CD to /var/home/ftp/pub.

To download optional language files

1. Insert the optional language CD in your laptop's CD-ROM drive.
2. On the Maintenance Web Interface, under Miscellaneous, select **Download Files**.

Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool

3. Select the **Files to download from the machine I'm using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click the **Download** button.

When the transfer is complete, the message

Files have been successfully downloaded to the server

is displayed.

6. If more than four optional language files need to be downloaded, repeat this procedure.

Copies of the optional language files are now in the **/var/home/ftp/pub** directory and will be automatically installed during the upgrade process.

Creating an IA770 test message for the upgrade

To test IA770 after the upgrade

1. Write down the number of a test voice mailbox, or create one if none exists.
2. Write down the number of the IA770 hunt group.
3. Leave a message on the test mailbox that will be retrieved after the upgrade.

Shutting down IA770

To shut down IA770

Note:

If you are using the Avaya Installation Wizard (IW) to upgrade the server, skip this procedure. The IW will execute the **stop** command automatically.

1. Type **telnet 192.11.13.6** and press **Enter**.
2. Log in as *craft* or *dadmin*.
3. Type **stop -s Audix** and press **Enter** to shut down AUDIX. Note that the "A" in Audix must be capitalized.

The shutdown will take a few minutes.

4. Type **watch /vm/bin/ss** and press **Enter** to monitor the shutdown.

The watch command will automatically refresh every few seconds. When the shutdown is complete, you will see only the voicemail and audit processes. For example:

voicemail:(10)

audit http:(9)

Press **Ctrl+C** to break out of the **watch** command.

5. Type `/vs/bin/util/vs_status` and press **Enter** to verify that AUDIX is shut down.

When AUDIX is shut down, you will see

```
voice system is down
```



Important:

After upgrading an S8300, you must upgrade the G700 or G350 and media module firmware before restarting IA770.

To shut down IA770 with the Maintenance Web pages

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.



Important:

After upgrading an S8300, you must upgrade the G700 and media module firmware before restarting IA770.

Backing up S8300 recovery system files

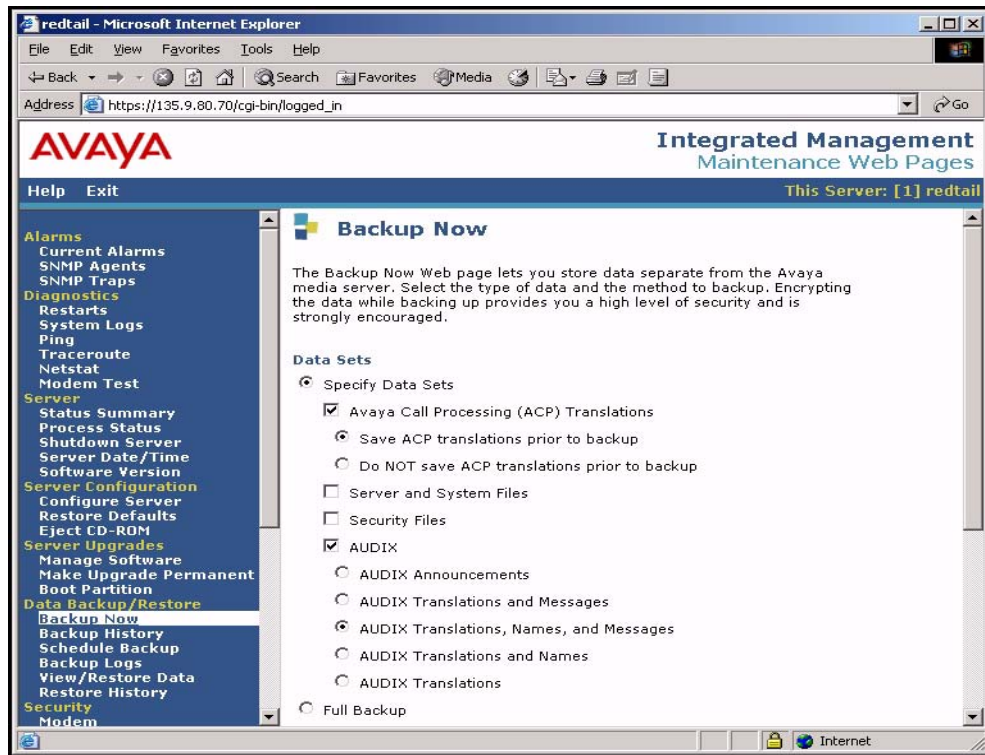
Before installing the S8300 software, back up the system data in case you need to back out of the upgrade. You should back up to an FTP, SFTP, or SCP server on the customer's network. To do this, you need an FTP, SFTP, or SCP address and directory path and a user ID and password to access the customer's network. Check with your project manager or the customer for this information. You can also back up the system data to the S8300 hard drive.

To back up S8300 recovery system data

1. Under Data Backup/Restore, click **Backup Now**.

The **Backup Now** screen displays.

Backup Now screen (Part One)



2. Select **Full Backup**, if available with the existing release, or select all data sets:

- Avaya Call Processing (ACP) Translations
- Save ACP translations prior to backup

Note:

Select ACP translations only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

- Server and System Files
- Security Files

3. If the AUDIX options are available, select AUDIX and select AUDIX Translations, Names, and Messages.



CAUTION:

Selecting the **Full Backup** radio button does NOT include AUDIX files. You must backup the IA770 INTUITY AUDIX data after you do the full backup.

Backup Now screen (Part Two)

4. Select the **FTP** for the backup method and fill in the appropriate fields with information provided by the customer.
5. Click **Start Backup** to back up the files.

Note:

The backup and restore processes use the ping service to check connectivity to the backup server. If a backup or restore operation fails, ensure that the ping service is enabled.

- i. On the Maintenance Web Interface, under **Security** select **Firewall**.
- ii. In the **Service** column, find **ping**.

The checkboxes for both **Input to Server** and **Output from Server** should be checked.

6. To check the status of the backup:
 - a. Under **Data Backup/Restore**, click **Backup History**.
 - b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

When the backup is finished, the **Backup History Results** screen displays

The final status for your backup job is shown below.

For each backup set, the message

BACKUP SUCCESSFUL

displays, if the set was backed up successfully.

7. If the AUDIX options are available, repeat Steps 3–6 for AUDIX Announcements.

Copying the service pack files to the media server (starting from R2.x only)

Note:

Do not perform this task if you are upgrading an R3.0 release to R4.0.

To copy service pack files to the media server from the laptop

1. On the Maintenance Web Interface, under Miscellaneous, click **Download Files**.
2. Select the download method, "Files to download from the machine I'm using to connect to the server."

Note:

Do not select the checkbox, "Install this file on the local server."

3. Browse to the directory on the laptop that contains the pre-upgrade and post-upgrade service pack files.
4. Select the service pack files and click **Download**.

Installing the pre-upgrade software service pack (starting from R2.x only)

Note:

Do not perform this task if you are upgrading an R3.0 release to R4.0.

A pre-upgrade service pack is required to modify the server upgrade tools, including the web Interface and upgrade scripts, which will enable the upgrade to Communication Manager 4.0 to complete successfully. LSPs with R2.x software also require the pre-upgrade service pack.

To install the pre-upgrade service pack

1. On the Welcome page of the Communication Manager Web pages, select **Launch Upgrade Tool**.

The Upgrade Tool Welcome page appears.

2. Select **Schedule Upgrade** from the menu on the left pane.

The Schedule Upgrade page appears.

3. Enter the file name of the pre-upgrade software service pack in the **Update File Name** field for the **Main Server(s)**.
4. Enter the file name of the pre-upgrade software service pack in the **Update File Name** field for **LSP**.

5. Scroll down to the **Main Server Targets** field and select the **Update** box for the primary controller.
6. Scroll down to the **LSP Targets** field and select the **Update** box for the LSPs you are upgrading.
7. Click **Run Now**.

The Upgrade Tool updates the primary controller and any LSPs you selected.

8. Check the status of the updates by selecting the **View Current** option from the left pane menu.

The word Completed appears in the status field for the primary controller and each LSP you are updating.

Copying Files to the S8300 hard drive

You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Post-upgrade software service pack
- License file
- Avaya authentication file
- New firmware files
- Security updates
- IA770 service packs or RFUs

To copy files to the S8300 hard drive

1. Under **Miscellaneous** on the Maintenance Web pages, click **Download Files**.

Download Files screen

Download Files

The Download Files Web page lets you download files to the media server.

☒ File(s) to download from the machine I'm using to connect to the server

☐ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

☐ Install this file on the local server

**If the above box is checked, you may specify only one file for downloading.

2. Select "Files to download from the machine I'm using to connect to the server" and browse to each file you want to copy to the S8300. Leave the "Install this file on the local server" checkbox **unchecked**.

If you need to download an IP Telephone firmware file, download this file last with the "Install this file on the local server" checkbox **checked**.

Note:

To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to `pub` after starting ftp and logging in; that is, type `cd pub`.

3. Click on **Download** to copy the files to the S8300. The transfer is complete when you see the message,

Files have been successfully uploaded to the server



Important:

Remove the Communication Manager software distribution CD from the DVD/ CD-ROM drive.

Copying authentication files to the LSPs

The Upgrade Tool cannot install authentication files. Therefore, copy the authentication files to a computer that can connect to the customer's network. From that same computer, log into the Web pages for each LSP and use the Download Files screen to download the authentication file (see [Copying Files to the S8300 hard drive](#) on page 273).

Copying the Communication Manager software and media gateway firmware to a TFTP or HTTP server

If you want to remotely copy Communication Manager software to LSPs *without* physically inserting the CD-ROM into the CD-ROM drive of each LSP, you must post the software on the TFTP or HTTP server you set up earlier. To post the software, use whatever tools are available in the customer's network for file transfer.

If there are media gateway firmware files that you are installing that are more recent than those on the Software CD-ROM, post these individual files on a TFTP server. This TFTP server can be the /tftpboot directory of an S8300 Media Server.

Copying the Communication Manager software and media gateway firmware to the server

Normally, during an upgrade of the primary controller, you will have the Communication Manager Software Distribution CD-ROM that contains the latest software to install. The latest software for the S8300 has a file name that reflects the most recent load of software (*For example only*, 013-01.0.640.1). The latest service pack software for Communication Manager also reflects the most recent load of software (*for example only*, 03.1-01.0.640.0).

These files also contain the most recent firmware for the G700 Media Gateway, the various media modules, and the P330 Stack Processor.

Preparing LSPs

If you are upgrading any LSPs using the Upgrade Tool from the primary controller, you must copy the Communication Manager software to the LSP itself before running the upgrade. You can copy the files from any of the following:

- The CD-ROM
- A TFTP server. See [Setting up a TFTP server or HTTP server for LSP software download, if desired](#) on page 259.
- An HTTP server using a URL. See [Setting up a TFTP server or HTTP server for LSP software download, if desired](#) on page 259.

If you use a CD-ROM, you or someone else must be physically on-site with each LSP to insert and remove the CD-ROM.

If you use a TFTP or HTTP server, you can copy software to each server remotely. However, the WAN must be able to handle files requiring large bandwidth, up to 71 MB for a single file. The download from TFTP or HTTP server may experience a timeout, in which case you must restart the download.

To transfer software files to the server



CAUTION:

When you are upgrading the media server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the media server to a release that is not supported as an upgrade path, you might corrupt the translations.

Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.

To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access <http://support.avaya.com>. Select **Downloads > Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates > Latest Communication Manager Software & Firmware Compatibility Matrix**.

1. Do one of the following steps:
 - a. If using a CD-ROM as a software source, insert the Communication Manager software distribution CD into the CD-ROM drive. Go to step [3](#).
 - b. If using a TFTP or HTTP server, log in to the S8300 Linux interface. For LSPs, this can be a remote log in. Go to step [2](#).
2. To check for a connection to the TFTP or HTTP server, type `ping ip_address` where *ip_address* is the address of the TFTP or HTTP server, and press **Enter**.
Replies from the server scroll down the screen.
3. Log in to the S8300 Web interface. For LSPs, this can be a remote log in.
4. If using a TFTP or HTTP server for software download, do the following steps to verify the LAN/WAN connections are open for file exchange. Otherwise go to step [5](#).
 - a. Click **Firewall** on the Maintenance Web page menu.
The Firewall screen appears.

- b. Check that **tftp** Service using Port/Protocol **69**, or **http** Service using Port/Protocol **80**, is checkmarked in both **Input to Server** and **Output to Server** columns. Go to step [5](#).
5. Under Server Upgrades, click **Manage Software**.

The **Manage Software** screen appears.

Manage Software screen

Manage Software

Progress: Choose Task

Choose Task This server is currently running release: **S8300-013-01.0.637.0**

Select the task to perform and click **Continue**.

☐ Copy a release to the local hard drive, but do not install it.

☐ Install one of the following releases currently resident on the local hard drive:

- **03.0-01.0.636.0**
- **03.0-01.0.637.0**

☐ Delete one of the above releases from the local hard drive.
(This does not affect the release that is running on the system.)

Note: If the web session times out, you can recover by logging in again and clicking the Manage Software link from the menu.

Continue **Cancel** **Help**

6. Select the radio button **Copy a release to the local hard drive, but do not install it**.

Note:

The S8300 hard drive can hold up to three releases without having to delete a release before copying a new release from the Communication Manager software distribution CD.

The S8300 displays the **Choose Source** screen, which allows you to copy files from one of several possible sources to the S8300 hard drive.

Choose Source screen

Manage Software: Copy

Progress: Choose Source

Choose Task
Choose Source
Choose Software
Copy in Progress
Copy Complete

These pages allow you to copy a new release to the local hard drive without installing it. The directory structure for the source of the copy must have the same directory structure as the software distribution CD-ROM.

This server is currently running release: **S8300-012-01.0.309.0**

The following releases are resident on the hard disk:

- No releases are resident

Select the place to copy from:

☐ Copy from this server's CD-ROM drive:

☐ Copy from TFTP server at this IP address:

☐ Copy from URL:

Proxy Server: (e.g proxy.domain:3152)

Note: If the web session times out, you can recover by logging in again and clicking the Manage Software link from the menu.

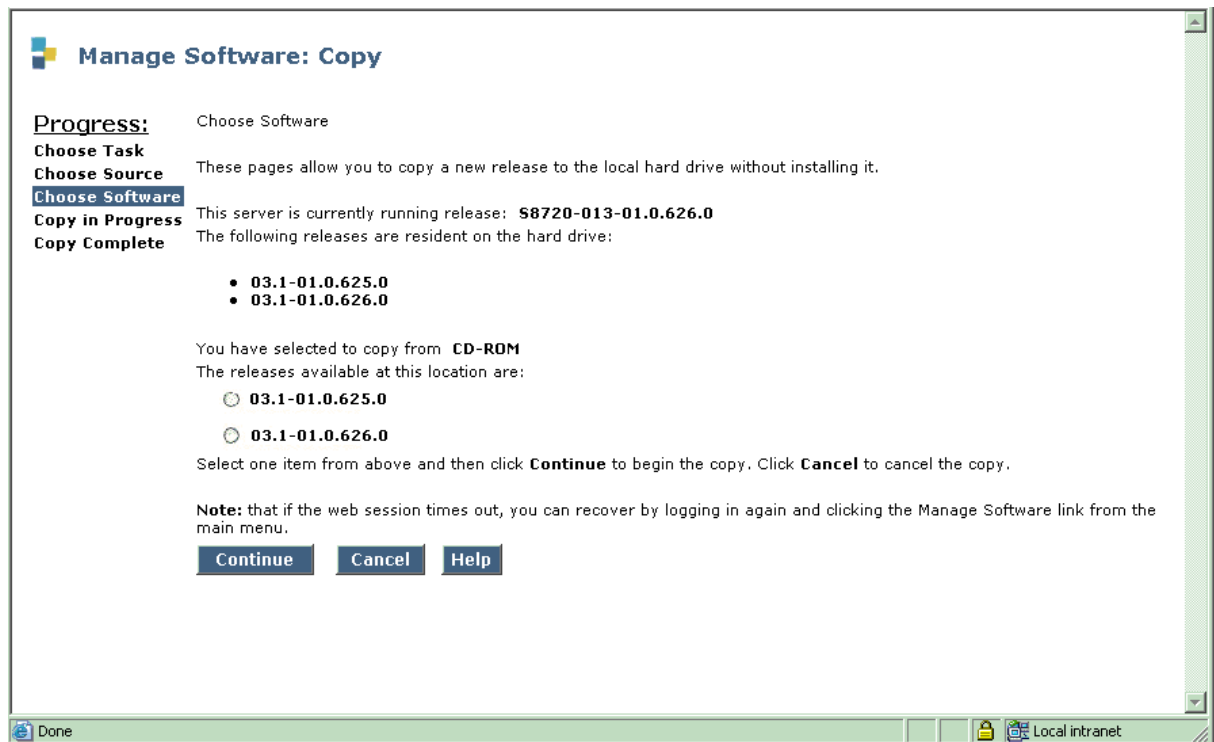
Possible sources include:

- This server's CD-ROM drive
- TFTP server at IP address (default is local laptop at 192.11.13.5)
- IP address or URL specified in **Copy from URL:** field, including the subdirectory /Releases. For example, if the URL is **http://denver-server.com**, then the complete URL will be **http://denver-server.com/Releases**.

If you select the **Copy from this server's CD-ROM drive:** radio button, all available CD drives are checked. The first drive found with a valid release is used, in the event multiple CD drives are actually present. If you select

The **Choose Software** screen displays.

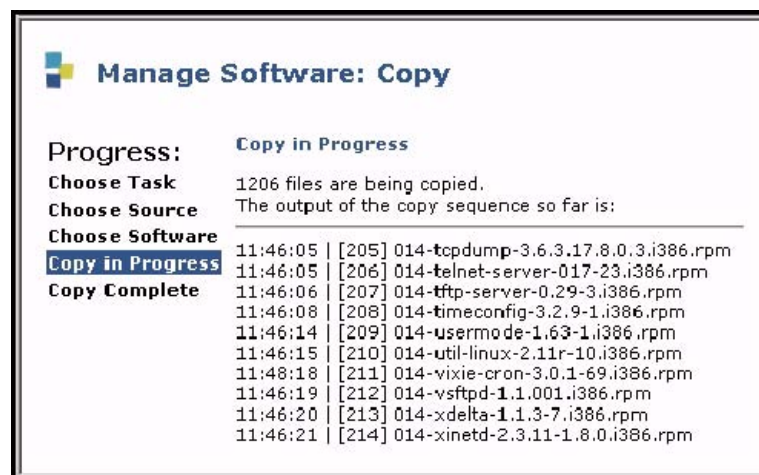
Choose Software screen



The screen is presented with no radio button selected.

7. Select the release to be copied and click **Continue**. The **Copy in Progress** screen displays.

Copy in Progress screen



The screen lists each file as it is being copied to the S8300 hard drive. When the copy completes successfully, the **Copy Complete** screen displays.

Copy Complete screen



This screen indicates the release just copied, shows the release running on the S8300, and shows the releases resident on the server's hard drive.

Note:

Did you experience a timeout while downloading from a TFTP or HTTP server? If so, you must restart the download.



CAUTION:

At this point you are finished with copying the software to the server. If the software was on CD-ROM, **remove the CD from your laptop now** to avoid possible problems the next time your laptop is rebooted.

8. Repeat this procedure for each LSP you want to upgrade with the Upgrade Tool.

Obtaining additional data for running the Upgrade Tool

To run the Upgrade Tool for upgrading media gateways, you need the following from the customer:

- Logins and passwords for the media gateways, including global logins and passwords and individual media gateway logins and passwords.
- IP addresses for any TFTP servers being used.

You can use the worksheets in the *Job Aid: Upgrade Tool and Worksheets*, 555-245-757, to capture this information.

Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways

This section describes the procedures to use the Upgrade Tool to upgrade the S8300 Media Server to Communication Manager release 4.0, including its LSPs and G700 media gateways.

This procedure also applies to the upgrade of the G350 and G250-series Media Gateways and includes the following tasks:

- [Checking the current releases of all devices \(optional\)](#) on page 281
- [Running the upgrade](#) on page 284
- [Viewing the status of the upgrade in progress](#) on page 286
- [Installing updated authentication files](#) on page 290
- [Saving translations](#) on page 291
- [Setting rapid spanning tree on the network](#) on page 293

Checking the current releases of all devices (optional)

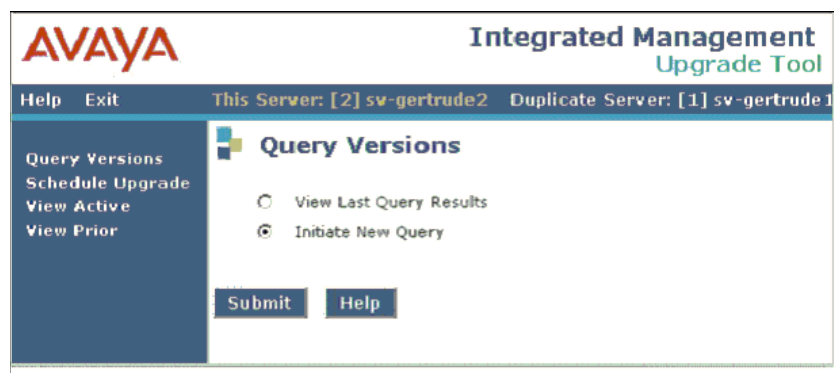
You should check the current releases of all devices (LSPs, media gateways, and media modules) to verify which devices need to be upgraded. This step, while optional, can speed the upgrade process if you find that some devices do not require upgrades.

1. On the Welcome page of the Communication Manager Web pages, select **Launch Upgrade Tool**.

The Upgrade Tool Welcome page appears.

2. Select **Query Versions** from the menu on the left pane.

The Query Versions Select page appears.



3. Select **Initiate New Query** and click **Submit**.

It could take several minutes to complete a new query. The time a new query takes depends on the number of LSPs and gateways that are in the configuration. The system automatically finds and lists the primary controller, LSPs, and G700 Media Gateways registered with the primary controller. Additionally, the media modules are listed for each media gateway.

Because of the potential length of this screen, hot links are provided in each section so you can jump to the other sections.

The screenshot shows the Avaya Integrated Management Upgrade Tool interface. The top header includes the Avaya logo and the title "Integrated Management Upgrade Tool". Below the header, there is a navigation bar with "Help" and "Exit" links, and a status bar indicating "This Server: [1] pilsner1".

The main content area is titled "Query Versions" and contains several sections:

- Query Versions**: A sidebar menu with options: "Query Versions", "Schedule Upgrade", "View Active", and "View Prior".
- Main Server Targets**: A table with columns "Node Name", "IP Address", and "Query?". It lists "pilsner1" with IP "125.9.72.1" and a checkbox for "Query?".
- LSP Targets**: A table with columns "Node Name", "IP Address", and "Query?". It lists "mg6-lsp" with IP "122.16.22.62" and a checkbox for "Query?".
- Common G350/G700 Logon Values**: A section with a note "(These values will be used unless an override is specified below)". It contains input fields for "Logon ID" and "Password".
- Override Common Values for G350 Targets**: A section with a note "(The common G350/G700 Logon and Password Server Values will be used for all values left blank.)". It contains a table with columns "Node Name", "IP Address", "Query?", "Logon ID", and "Password". It lists "MG60 - G350" with IP "122.16.22.65" and a checked checkbox for "Query?".
- Override Common Values for G700 Targets**: A section with a note "(The common G350/G700 Logon and Password Server Values will be used for all values left blank.)".

At the bottom of the main content area, there are buttons: "Query", "Save", "Select All", "De-select All", and "Help".

Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways

4. Enter data for the devices you want to query.

You can select to query all of the devices or you can select individual devices. Enter a common login ID and password that can be used to access all the gateways that do not have an override value entered. You can save your entries on the screen and return to the screen later to run the query. This allows you the capability to stop and research any necessary information without losing your entries.

5. When you are finished with your selections, click **Query**.

The Query Results screen appears.

The screenshot shows the Avaya Integrated Management Upgrade Tool interface. The title bar includes the Avaya logo and the text "Integrated Management Upgrade Tool". Below the title bar, there is a status bar showing "This Server: [1] sv-gertrude1 Duplicate Server: [2] sv-gertrude2". The main window is titled "Query Versions Results" and contains a table with the following columns: Node Name, IP Address, Type, Vintage, Slot, Current Version, Update Version, Platform / Security Version, and SID MID. The table lists various devices and their versions, including sv-mg2-lsp, sv-gertrude-g350B, sv-MG2-860, sv-gertrude1, and sv-gertrude2. The "Query Status" is displayed as "Complete" in green text. A "Help" button is located at the bottom left of the main window.

Node Name	IP Address	Type	Vintage	Slot	Current Version	Update Version	Platform / Security Version	SID	MID
sv-mg2-lsp	182.168.222.20	LSP			S8300-013-00.0.335.0				
sv-gertrude-g350B	182.22.21.23	G350 (processor)							
		MM722	1	v2	2				
		MM720	3	v3	6				
		MM712	3	v4	5				
		MMANALOG		v7	62				
		Device Manager			2.1.6				
sv-MG2-860	182.168.222.21	G700 (MGP)			24.7.0				
		MM760		v0	203				
		MM712	3	v2	5				
		MM710	2	v3	9				
		MM710	2	v4	9				
		Cajun Stack			4.1.1				
		Device Manager			4.6.2				
sv-gertrude1	182.22.22.172	main			S8710-013-00.0.332.0	00.0.332.0-1706		1	1
sv-gertrude2	182.22.22.173	main			S8710-013-00.0.332.0	00.0.332.0-1706		1	1

Query Status: Complete

Help

6. Note the devices that do not require updates, if any.

Running the upgrade

Follow these steps:

- 1. To set up and schedule upgrades, click **Schedule Upgrade**.

The Schedule Upgrade screen appears. At the bottom of the screen, the system displays all main servers, LSPs, and gateway targets that are administered.

Query Versions

Schedule Upgrade

View Active

View Prior

Schedule Upgrade

Scroll to: [Server Targets](#) [Common Values](#) [G350 Overrides](#) [G700 Overrides](#)

Software/Firmware/Update

Target	Upgrade File Name	Update File Name	Platform/Security File Name
Main Server(s)			
ESS Server(s)			
LSP			

G350 Media Gateway File Names

G350 (processor)	
Device Manager	
MM312 (DCP)	
MM710 (T1/E1)	
MM711 (analog) (HW v <= 6)	
MM711 (analog) (HW v = 7)	
MM711 (analog) (HW v >= 20)	
MM712 (DCP)	
MM714 (analog)	
MM716 (24 Port analog)	

ScheduleRun NowSaveSelect AllDe-select AllHelp

- 2. Fill in all appropriate fields. Click **Help** for information about the fields on the screen.

Note:

The file names must be entered in the correct format. Do not change the names of the firmware files in the process of loading them onto the TFTP servers. See [Firmware file formats](#) on page 205.

Use the information from the planning forms or Upgrade Worksheets to complete the Software/Firmware fields.

Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways

Use the following guidelines to setup the upgrade:

- If the customer uses a common logon ID and password for multiple gateways, complete the **Common G350/G700 Logon Values** fields.
- If the customer has a centralized TFTP server for use by multiple G700 or G350 Media Gateways or the customer has a centralized FTP server for use by multiple G350 Media Gateways, complete the **Common TFTP/FTP Server Values** fields.
- Use the **Max Sessions** field to specify how many gateways can be simultaneously connected to a TFTP or a FTP server for upgrading. The number must be between one and 20 inclusive. If you do not specify a number, the Upgrade Tool defaults to six.
- If any gateways require unique logon values or unique TFTP servers, complete the **Override Common Values for G350 and G700 Targets** fields. You can enter override values for the following:
 - The IP address of the unique TFTP server.
 - The completed path to the directory from the root of the TFTP server.
 - The logon information for the gateway.
- If any override fields are left blank, the values entered in the Common fields are used.
- Some upgrades may time out due to network traffic and limitations on how long the Upgrade Tool will allow an upgrade to continue. The upgrade of a single LSP has a limit of one hour. The upgrade of a media gateway has a limit of 30 minutes.
- Since the media gateway (MGP) firmware files are fairly large they may cause a timeout during an upgrade to a remote location. What you enter in the TFTP Directory field depends on the type of TFTP server you are using. If the TFTP server is:
 - An S8300 or an LSP, enter the path to the firmware files relative to the /tftpboot directory. For example, if the firmware files are in /tftpboot/cm3.0/318.0, enter **cm3.0/318.0**.

Note:

If the files are in the /tftpboot directory on the S8300 server/LSP and there is no subdirectory, leave the TFTP Directory field blank.

- An Avaya Windows server, enter the path of the outbound source for the TFTP server specified to be accessed. For example, if the firmware files reside in the directory c:ftp_outbound\cm3.0\340.3 and the TFTP server application is configured to have its outbound source as c:ftp_outbound, then you would enter cm3.0\340.3 as the value in the TFTP Directory field.

Note:

If the files are in /tftpboot directory on the Avaya server and there is no subdirectory, leave the TFTP Directory field blank.

- A customer server, ask the customer how their TFTP server is set up.

Note:

A TFTP server must be accessible over the LAN from the gateway you are upgrading.

3. Click **Schedule** to set up the upgrade schedule or **Run Now** to run the upgrades immediately.

Viewing the status of the upgrade in progress

To review the status of an upgrade in progress, click **View Active**.

Note:

If you use the View Active screen while upgrading the server on which the Upgrade Tool itself is running, the screen displays an error while the server is rebooted. To view the successful status of the upgrade of the server on which the Upgrade Tool is running, you must use the View Prior screen after the upgrade is complete.

However, the upgrade is not complete until the following events occur:

- The server reboots.
- Additional database updates occur after the reboot.
- The upgrade is made permanent.

Making the upgrade permanent takes at least an additional five minutes beyond the reboot. You can check to see when the upgrade is complete by checking the View Prior upgrade screen periodically or by doing the following:

1. Access the Maintenance Web pages on the server from which you started the upgrade.
2. Select **Boot Partition**.
3. Check to see if a physical partition is identified as both the boot partition and the active partition, and that the physical partition contains the most recent software release.

Note:

The Upgrade Tool automatically makes the upgrade permanent.

Note:

This Web session will be interrupted by the reboot that occurs during the primary server upgrade. After the reboot, the links in the main menu of the Web interface will not function. Therefore, you must close and reopen the Web browser to continue with the upgrade procedure.

4. Close the Web browser.
5. Reopen the Web browser and log in.

Creating a customer login, if necessary

CAUTION:

A customer superuser login must exist *before* you install an authentication file. If you did not check for the login (see [Ensuring a super-user login exists](#) on page 252, you must create one before you install the new authentication file.

To create a login:

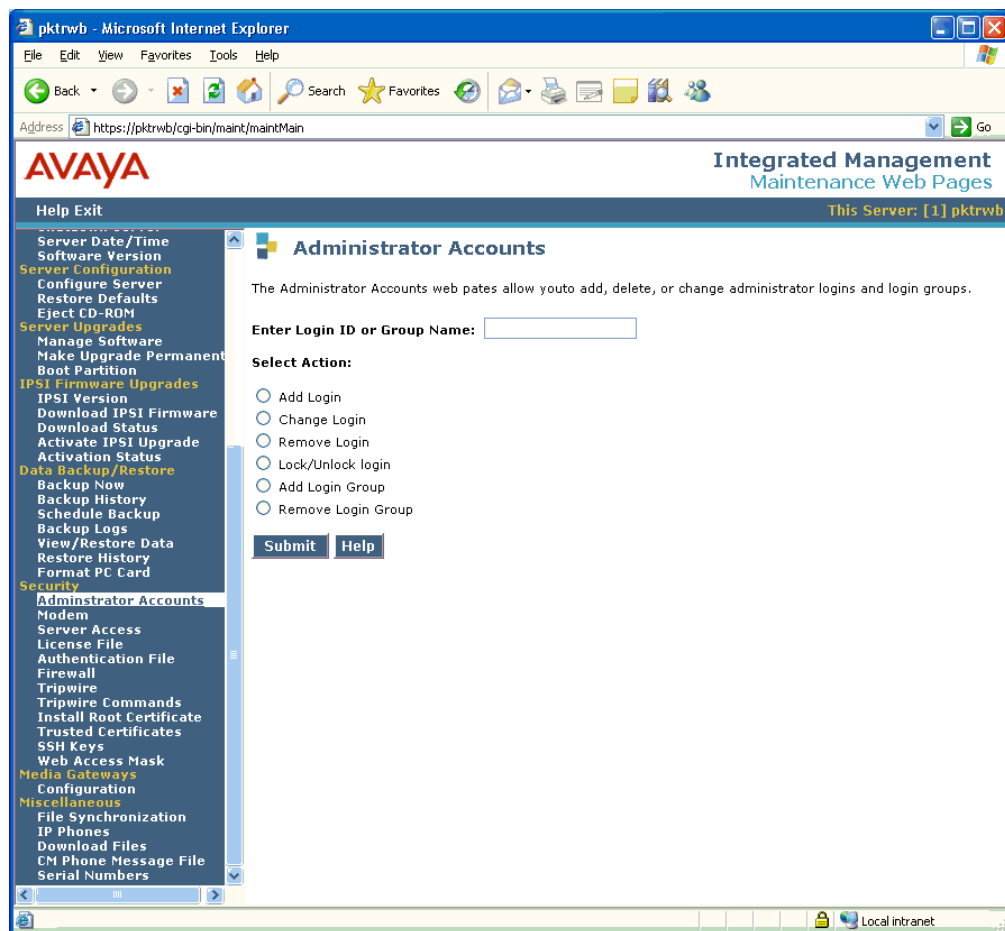
1. Ask a customer representative for a login name and password that the customer would like for the superuser login.

Note:

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

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool

3. Type the login name in the **Enter Login ID or Group Name** field.
4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot displays the Avaya Integrated Management Maintenance Web Pages interface. The top header shows the Avaya logo and the title 'Integrated Management Maintenance Web Pages'. Below the header, a navigation menu on the left lists various system management tasks, including 'Restore Defaults', 'Eject CD-ROM', 'Server Upgrades', 'Pre Upgrade Step', 'Manage Software', 'Make Upgrade Permanent', 'Boot Partition', 'Manage Updates', 'IPSI Firmware Upgrades', 'IPSI Version', 'Download IPSI Firmware', 'Download Status', 'Activate IPSI Upgrade', 'Activation Status', 'Data Backup/Restore', 'Backup Now', 'Backup History', 'Schedule Backup', 'Backup Logs', 'View/Restore Data', 'Restore History', 'Format CompactFlash', 'Security', 'Administrator Accounts', 'Modem', 'Server Access', 'Syslog Server', 'License File', 'Authentication File', 'Firewall', 'Tripwire', 'Tripwire Commands', 'Install Root Certificate', 'Trusted Certificates', 'SSH Keys', 'Ethernet Switch Ports', and 'Web Access Mask'. The main content area is titled 'The Administrator Logins -- Add login web page allows you to add a new administrator login.' and contains the following fields and options:

- Login ID:** Pre-filled with 'randy'.
- login group:** Text input field containing 'susers'.
- additional groups:** Text input field containing 'prof18'.
- allow Linux shell access:** A checkbox that is currently unchecked.
- lock this account:** A checkbox that is currently unchecked.
- date (YYYY-MM-DD) on which account is disabled (blank to ignore):** An empty text input field.
- select type of authentication:** Radio button options for 'password' (selected) and 'ASG'.
- enter key or password:** An empty text input field.
- re-enter key or password:** An empty text input field.
- force password/key change on first login:** Radio button options for 'yes' and 'no' (selected).
- maximum Number of days a password may be used (PASS_MAX_DAYS):** Text input field containing '90'.
- minimum number of days allowed between password changes (PASS_MIN_DAYS):** Text input field containing '90'.
- minimum acceptable password length (PASS_MIN_LEN):** Text input field containing '8'.
- number of days warning given before a password expires (PASS_WARN_AGE):** An empty text input field.
- days after password expires to lock account (0=immediate):** An empty text input field.

At the bottom of the form, there are 'Add' and 'Help' buttons. The status bar at the very bottom shows 'Done' and 'Internet' connectivity.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

Run the Upgrade Tool to upgrade the primary controller, LSPs, and G700 media gateways

10. Complete the following fields:

- enter key or password
- re-enter key or password
- force password/key change on first login



CAUTION:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

Installing updated authentication files

CAUTION:

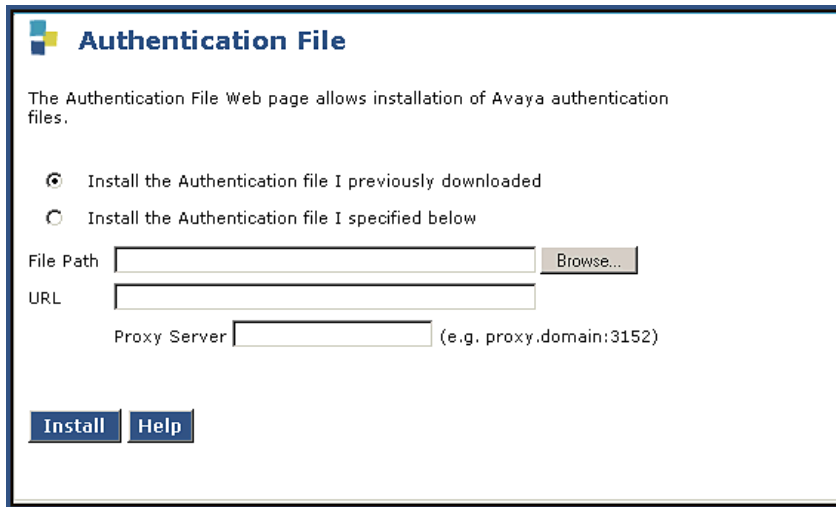
A super-user login, dadmin or another customer superuser login, must exist *before* you install an authentication file. If the authentication file does not install, you might need to create a super-user login, then install the new authentication file. See [Ensuring a super-user login exists](#) on page 252.

Log into each LSP remotely if possible, and then the primary controller, to install the authentication files:

1. On the Maintenance Web Interface menu under Security, select **Authentication File**.

The **Authentication File** screen displays.

Authentication File screen



2. Select **Install the Authentication file I previously downloaded** and click **Install**.

The system tells you the authentication file is installed successfully

If upgrading an LSP, synchronize translations from the primary controller

If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

1. Log in with `telnet` or `ssh`.
2. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`
3. Type `start -cf`

Saving translations

Note:

If the S8300 you are upgrading is an **LSP**, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session. and log in as *craft* (or *dadmin*).
2. If the S8300 you are upgrading is a primary controller, at the SAT prompt, type `save translation` and press **Enter**.
3. If the S8300 you are upgrading is an LSP, then on the primary controller, type `save translation lsp` and press **Enter**. This command distribute saved translations out to the LSPs.

When the save is finished, the system displays the message,

`Command successfully completed.`

The system automatically performs a reset system 4. If you are upgrading an LSP, you are logged out.

Ensuring the MGP default gateway IP address is set

Communication Manager release 4.0 *requires* that the built-in VoIP module of the G700 Media Gateway has a default gateway IP address. To ensure that this IP address is set, perform the following steps:

1. Log into the G700 Media Gateway console port (see [Logging in to the P330 Stack Processor with a Direct Serial Connection](#) on page 64).
2. Type `configure` to obtain the **P330-1(configure)#** prompt.
3. At the **P330-1(configure)#** prompt, type `session mgp`.

4. At the **MG-???-1(configure)#** prompt, type **show ip route mgp**.

The list of mgp routes appears.

```
MG-001-1(super)# show ip route mgp
```

DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	135.9.80.254	motfec0	(3/0/165)
135.9.80.0	255.255.255.0	135.9.80.88	motfec0	(101/0/0)

```
MG-001-1(super)#
```

5. Check that a Gateway IP address exists for Destination 0.0.0.0.
6. If a Gateway IP address does not exist, type, at the **MG-???-1(configure)#** prompt, **set ip route 0.0.0.0 0.0.0.0 <IP_address>**, where **<IP_address>** is the default gateway IP address.

After you reboot the media gateway, the IP address is active and available.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 Stack Processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 Stack Processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330 Stack Processors now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop. To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330T User's Guide* (available at <http://www.avaya.com/support>).

Post-upgrade tasks

After the upgrade is complete, perform the following post-upgrade tasks:

- [Installing IA770 service pack \(or RFU\) files, if any](#) on page 294
- [Copying IP Phone firmware to the media server, if necessary](#) on page 297
- [Restoring the 4600-series phone configuration file, if any](#) on page 298
- [Completing the upgrade process \(S8300 is the primary controller\)](#) on page 298

Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update

After the upgrade is complete, perform the following post-upgrade tasks.

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing IA770 service pack (or RFU) files, if any

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at <http://support.avaya.com>.

1. Select **Messaging Administration** from the main menu.
2. Select **Utilities** from the Messaging Administration menu.
3. Select **Software Management** from the Utilities menu.
4. Select **Advanced Software Installation** from the Software Management menu.

5. Select **Continue this operation without current system backup**.
6. Select the IA770 update package and click **Install Selected Packages**.

Note:

The system automatically prompts you to restart INTUITY AUDIX when the service pack has been installed. Therefore, if you restart AUDIX at this time, you do *not* need to perform the following procedure, [Starting IA770 INTUITY AUDIX Messaging](#).

Starting IA770 INTUITY AUDIX Messaging



CAUTION:

You do *not* need to perform this task if you restarted AUDIX as a part of the installation of the IA770 service pack.

After the IA770 INTUITY AUDIX Messaging application has been updated, you must restart it using the following steps:

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Start Messaging Software**.

The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Verifying start up of IA770 INTUITY AUDIX Messaging

To verify operation of IA770 INTUITY AUDIX Messaging, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

the **View Process Status Results** screen displays.

View Process Status screen



Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

[Help](#)

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an IA770 sanity test:
- At the Linux command line, type `/vs/bin/display`
 - All states should be `Inserv` with an associated phone number.
 - Retrieve the test message saved before the upgrade.

Saving translations

To save translations:

- In the SSH session, open a SAT session.
- Log in again as *craft*.

3. Type **save translation** and press **Enter**.

When the save is finished, the system displays the message,
Command successfully completed.

If using IA770, administering switch integration for H.323

The IA770 INTUITY AUDIX Messaging application uses H.323 signaling instead of the CWY1 board for integration with Communication Manager. The tasks for administering the H.323 integration are explained in *Administering Media Servers to work with IA770*.

Testing to verify system functionality

Test the system for functionality, if you are upgrading an S8300 primary controller;

1. Verify the following:
 - Telephones have dial tone
 - You can call from one telephone to another telephone on the system
 - You can make an external trunk call.
 - The media gateways have registered. Use the SAT command **list media-gateway**.

Copying IP Phone firmware to the media server, if necessary

If, before the upgrade, the server was serving as an http server for IP phone firmware, download the most recent IP phone firmware bundle available from the Avaya Firmware Download Web site. The firmware bundle reinstates the 46xx IP Phone Web page in Communication Manager and also makes the 46xx IP Phone firmware for the tftp or http server capability of the media server.

Note:

The IP phone firmware that was originally downloaded will have been overwritten.

To copy files to the media server:

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

4. Click **Install this file on the local server**.
5. Click **Download** to copy the file(s) to the media server.

The files are copied automatically to the /tftpboot directory. The 46xx IP Phone Web page is reinstated at the next reboot.

Restoring the 4600-series phone configuration file, if any

If you copied a 4600-series phone configuration file to the **/var/home/ftp/pub** directory prior to the upgrade, you should restore it after the upgrade. However, before you restore the file, be sure you have downloaded the appropriate IP phone firmware.

1. At the Linux command line, type `cd ~ftp/pub`, and press **Enter**.
2. At the prompt, type `cp 46xxsettings.txt /tftpboot`, and press **Enter**.

The 4600-series phone settings file is now restored to the /tftpboot directory.

Completing the upgrade process (S8300 is the primary controller)

Complete the upgrade process with the following tasks:

1. [To check media modules](#) on page 298
2. [To enable scheduled maintenance](#) on page 299
3. [To busy out trunks](#) on page 299
4. [To check for translation corruption](#) on page 299
5. [To resolve alarms](#) on page 299
6. [To re-enable alarm origination](#) on page 299
7. [To back up the system](#) on page 299

To check media modules

1. Open a SAT session, and log in as *craft* (or *dadmin*).
2. Type `list configuration all` and press **Enter**.
3. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
4. Make test telephone calls to verify that Communication Manager is working.

To enable scheduled maintenance

1. Type `change system-parameters maintenance` and press **Enter**.
2. Ensure that the **Start Time** and **Stop Time** fields' administration is the same as before the upgrade.

To busy out trunks

1. Busy out trunks that were busied out before the upgrade (see [To record all busyouts](#) on page 262).

To check for translation corruption

1. Type `newterm` and press **Enter**.

If you do not get a login prompt and see the following message:

Warning: Translation corruption detected

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To resolve alarms

1. On the Maintenance Web Interface, under Alarms click **Current Alarms** to examine the alarm log.
2. If any alarms are listed, click **Clear All**.
3. Resolve new alarms since the upgrade through Communication Manager using the appropriate maintenance book.

To re-enable alarm origination

1. Telnet to the S8300 and log on.
2. At the command prompt, type `almenable -d b -s y`,
where
 - d b sets the dialout option to *both* (numbers)
 - s y enables SNMP alarm origination
3. Type `almenable` (without any options) to verify alarm origination enabled status.

To back up the system

1. Using the Maintenance Web Interface, back up the system as you did before the upgrade selecting **Save Translations** and all backup sets.

Upgrading an existing S8300B or S8300C to R4.0 using the Upgrade Tool

Chapter 6: Upgrading an existing G700 without an S8300 using the Upgrade Tool

This section covers the procedures to upgrade the firmware on an existing Avaya G700 Media Gateway without an Avaya S8300 Media Server. The G700 is controlled by an external primary server running Avaya Communication Manager. The primary server can be an Avaya S8500 or S8700-series Media Server or an S8300 residing in another G700.

Note:

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

About the existing G700 upgrade

To upgrade the firmware on an existing Avaya G700 Media Gateway without an Avaya S8300 Media Server, you perform the following major tasks:

1. [Before going to the customer site](#)
2. [On-site preparation for the upgrade](#)

The Upgrade Tool performs the following tasks automatically:

3. [Determining which firmware to install on the G700](#)
4. [Running the upgrade](#)

What are the G700 system components

A P330 Stack Processor is built into the G700 Media Gateway. (This processor is also known as the *Layer 2 switching processor*). In addition, the G700 contains:

- Media Gateway Processor (MGP)
- VoIP processor
- Up to four media modules
- Possibly an expansion module

Installing or upgrading the firmware for one or more of these processors and/or media modules is a required part of most new installations or upgrades.

About firmware files

You should obtain the firmware files for the G700 before going on-site. You can obtain the firmware files in bundled form on a CD or you can go to the Avaya Support website and download the individual firmware files onto your services laptop.

About the TFTP server

To install firmware on a G700 without an S8300 or LSP, you must first copy the firmware files to an external TFTP server on the customer LAN. The TFTP server can be a customer computer or it can be set up on your services laptop.

About system access

Accessing the G700

See [About connection and login methods](#) on page 41 for details on how to connect and log into the G700. You can access the G700 in several ways.

Direct connections

- If you are at the location of the primary server, you can connect directly to the Services port on the server and:
 - Open the Web Interface and use the Upgrade Tool.
 - Or, telnet to the server, and then telnet to the P330 stack processor
- If you are at the location of the G700, you can connect directly to the G700 Console port and open a Hyperterm session to access the P330 stack processor.

For direct connections, the TFTP server must be on the customer LAN; *not* on your laptop.

LAN connections

If you can connect to the customer's LAN, you can:

- Use your Internet Explorer browser to access the Web Interface on the primary server and use the Upgrade Tool.
- Telnet to the P330 stack processor and perform the installation commands.

For LAN connections the TFTP server either can be your laptop or a customer computer on the LAN.

Before going to the customer site

Perform the following tasks before going to the customer site:

- [Planning forms that the project manager provides](#) on page 303
- [Setting up the TFTP server on your laptop or on a customer PC, if necessary](#) on page 303
- [Downloading G700 firmware files to your TFTP directory](#) on page 304

Planning forms that the project manager provides

The project manager should provide you with forms that contain all the information needed to prepare for this installation. The information primarily consists of:

- IP addresses
- Subnet mask addresses
- Logins and passwords
- People to contact
- The type of system
- Equipment you need to install

Verify that the information provided by the project manager includes all the information requested in your planning forms.



Tip:

[Appendix B: Information checklists](#), provides several checklists to help you gather the installation and upgrade information.

Setting up the TFTP server on your laptop or on a customer PC, if necessary

A **tar.gz** file, which you obtain from a CD-ROM or a website, contains new G700 firmware. To install the firmware on a G700, you must place this **tar.gz** file on a TFTP server that is connected to the customer's LAN. The TFTP server can be a customer computer, or it can be your laptop, if you have arranged with the customer to connect your laptop to the LAN.

Note:

A Linux or Unix TFTP server should be used only if the customer already has an existing one. In these cases, you download the **tar.gz** file to your laptop and give it to the customer for proper placement and execution.

To obtain the TFTP server software and install it, see [Appendix D: Install the Avaya TFTP server](#).

Downloading G700 firmware files to your TFTP directory

To install new firmware for the G700 processors and the media modules, you first need to move the new firmware files to a directory on the TFTP server. The installation program reads the new firmware files from this directory on the TFTP server.

Perform one of the two procedures in this section, depending on whether you have a bundled tar.gz file on a CD or wish to download individual firmware files from the Avaya Support website.

Downloading individual firmware files

Download the firmware files from the Web to your TFTP directory

Note:

The sequence of links on the website may be somewhat different than described here.

1. Access the <http://www.avaya.com/support> website.
2. Navigate to Firmware Downloads for The G700 Media Gateway.

The system displays a list of firmware files.

3. Locate the file names that match the files listed in your planning documentation.

The file names will approximate those listed in [Table 14](#):

Note:

The latest firmware versions may differ from those listed in [Table 14](#). Also, the appropriate firmware version may depend on the hardware vintage and/or on the release of Communication Manager. See *Communication Manager Software/Firmware Compatibility Matrix* under Downloads on support.avaya.com.

**CAUTION:**

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Table 14: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_1_6.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.6.6.exe
G700 Media Gateway	mgp<version id>	mgp_24_21_1.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v57.fdl
8-port DCP Media Module	mm712<version id>	mm712v7.fdl
24-port analog Media Module	mm716<version id>	mm716v2.fdl
24-Port DCP Media Module	mm717<version id>	mm717v4.fdl
8-port/trunk Analog Media Module (version 6 or earlier)	mm711<version id>	mm711v17.fdl
8-port/trunk Analog Media Module (version 7)	mm711<version id>	mm711h7v24.fdl
8-port/trunk Analog Media Module (version 20 or later)	mm711<version id>	mm711h20v68.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v67.fdl
T1/E1 Media Module	mm710<version id>	mm710v14.fdl
8-port BRI Media Module	mm720<version id>	mm720v6.fdl
2-port BRI Media Module	mm722<version id>	mm722v2.fdl

- Double-click the file name.

The system displays a **File Download** window.

- Click on **Save this file to disk**.
- Save the file to the **C:\tftp** directory (or your alternate tftp location).
- Use WinZip or another zip file tool to unzip the file, if necessary.

On-site preparation for the upgrade

Before installing new firmware on the G700 processors and medial modules you need to prepare on-site by:

- [Accessing the P330 Stack Processor](#) on page 306
- [Verifying the contents of the tftpboot directory](#) on page 306

as described in this section.

Accessing the P330 Stack Processor

See [About connection and login methods](#) on page 41 for details on how to set up a connection and login.

Log on to the P330 Stack Processor using one of the following methods:

- Using a LAN connection, telnet to the IP address of the P330 Stack Processor and log in.
- If you are *not* using your laptop as the TFTP server, you can connect your Laptop directly to the G700 Console (Serial) Port. Then use HyperTerm or a similar terminal emulation application to log in to the P330 Stack Processor Command Line Interface (CLI).

You are now logged-in at the Supervisor level with prompt **P330-1(super)#**.

Verifying the contents of the tftpboot directory

Before proceeding with the G700 firmware installation, you should check the */tftpboot* directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the */tftpboot* directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.
2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the */var/home/ftp/pub* directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the *pub* directory.

3. Copy the firmware files from the *pub* directory to the */tftpboot* directory, using the S8300 Media Server command line interface.

To copy firmware files to the */tftpboot* directory of an S8300 Media Server, do the following:

- a. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
- b. Log in as *craft*.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to */var/home/ftp/pub*.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the */tftpboot* directory. To copy multiple firmware files (most firmware files have an *.fdl* suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the */tftpboot* directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to */tftpboot*.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

You should check the current releases of all devices (LSPs, media gateways, and media modules) to verify which devices need to be upgraded. This step, while optional, can speed the upgrade process if you find that some devices do not require upgrades.

1. From your laptop connected to the services port on the primary controller, launch the Web browser. You can also launch the Web browser over a LAN connection to the primary controller
2. On the services port connection, type **192.11.13.6** in the **Address** field to open the **Logon** page.
3. Log on as *craft* or *dadmin* when prompted.
4. Click **Launch Maintenance Web Interface** to get to the **Main Menu**.
5. On the Welcome page of the Communication Manager Web pages, select **Launch Upgrade Tool**.

The Upgrade Tool Welcome page appears.

Upgrading an existing G700 without an S8300 using the Upgrade Tool

6. Select **Query Versions** from the menu on the left pane.

The Query Versions Select page appears.



7. Select **Initiate New Query** and click **Submit**.

It could take several minutes to complete a new query. The time a new query takes depends on the number of LSPs and gateways that are in the configuration. The system automatically finds and lists the primary controller, LSPs, and G700 Media Gateways registered with the primary controller. Additionally, the media modules are listed for each media gateway.

Because of the potential length of this screen, hot links are provided in each section so you can jump to the other sections.

AVAYA Integrated Management Upgrade Tool

Help Exit This Server: [1] pilsner1

Query Versions

Scroll to: [Common Values](#) [G350 Overrides](#) [G700 Overrides](#)

Main Server Targets

Node Name	IP Address	Query?
pilsner1	125.9.72.1	☐

LSP Targets

Node Name	IP Address	Query?
mg6-lsp	122.16.22.62	☐

Scroll to: [LSP Targets](#) [G350 Overrides](#) [G700 Overrides](#)

Common G350/G700 Logon Values
(These values will be used unless an override is specified below)

Logon ID

Password

Scroll to: [Common Values](#) [LSP Targets](#) [G700 Overrides](#)

Override Common Values for G350 Targets
(The common G350/G700 Logon and Password Server Values will be used for all values left blank.)

Node Name	IP Address	Query?	Logon ID	Password
MG60 - G350	122.16.22.65	☒		

Scroll to: [Common Values](#) [LSP Targets](#) [G350 Overrides](#)

Override Common Values for G700 Targets
(The common G350/G700 Logon and Password Server Values will be used for all values left blank.)

8. Enter data for the G700 Media Gateways you want to query.

You can select to query all of the devices or you can select individual devices. Enter a common logon ID and password that can be used to access all the gateways that do not have an override value entered. You can save your entries on the screen and return to the screen later to run the query. This allows you the capability to stop and research any necessary information without losing your entries.

Upgrading an existing G700 without an S8300 using the Upgrade Tool

9. When you are finished with your selections, click **Query**.

The Query Results screen appears.

The screenshot shows the Avaya Integrated Management Upgrade Tool interface. The title bar includes the Avaya logo and the text "Integrated Management Upgrade Tool". Below the title bar, there is a status bar showing "This Server: [1] sv-gertrude1 Duplicate Server: [2] sv-gertrude2". The main content area is titled "Query Versions Results" and displays a table of system components and their versions. The table has columns for Node Name, IP Address, Type, Vintage, Slot, Current Version, Update Version, Platform/Security Version, and SID MID. The table lists various components including LSP, G350 (processor), MM722, MM720, MM712, MMANALOG, Device Manager, MG2-860, G700 (MGP), MM760, MM712, MM710, Cajun Stack, Device Manager, sv-gertrude1, and sv-gertrude2. The "Query Status" is displayed as "Complete" in green text. A "Help" button is located at the bottom left of the main content area.

Node Name	IP Address	Type	Vintage	Slot	Current Version	Update Version	Platform/Security Version	SID	MID
sv-mg2-lsp	182.168.222.20	LSP			S8300-013-00.0.335.0				
sv-gertrude-g350B	182.22.21.23	G350 (processor)							
		MM722	1	v2	2				
		MM720	3	v3	6				
		MM712	3	v4	5				
		MMANALOG		v7	62				
		Device Manager			2.1.6				
sv-MG2-860	182.168.222.21	G700 (MGP)			24.7.0				
		MM760		v0	203				
		MM712	3	v2	5				
		MM710	2	v3	9				
		MM710	2	v4	9				
		Cajun Stack			4.1.1				
		Device Manager			4.6.2				
sv-gertrude1	182.22.22.172	main			S8710-013-00.0.332.0	00.0.332.0-1706		1	1
sv-gertrude2	182.22.22.173	main			S8710-013-00.0.332.0	00.0.332.0-1706		1	1

Query Status: Complete

Help

10. Note the devices that do not require updates, if any.

Running the upgrade

Follow these steps:

1. To set up and schedule upgrades, click **Schedule Upgrade**.

The Schedule Upgrade screen appears. At the bottom of the screen, the system displays all main servers, LSPs, and gateway targets that are administered.

Schedule Upgrade

Scroll to: [Server Targets](#) [Common Values](#) [G350 Overrides](#) [G700 Overrides](#)

Software/Firmware/Update

Target	Upgrade File Name	Update File Name	Platform/Security File Name
Main Server(s)			
ESS Server(s)			
LSP			

G350 Media Gateway File Names

G350 (processor)	
Device Manager	
MM312 (DCP)	
MM710 (T1/E1)	
MM711 (analog) (HW v <= 6)	
MM711 (analog) (HW v = 7)	
MM711 (analog) (HW v >= 20)	
MM712 (DCP)	
MM714 (analog)	
MM716 (24 Port analog)	

Schedule Run Now Save Select All De-select All Help

2. Fill in all appropriate fields for the G700 Media Gateway. Click **Help** for information about the fields on the screen.

Note:

The file names must be entered in the correct format. Do not change the names of the firmware files in the process of loading them onto the TFTP servers. See [Firmware file formats](#) on page 305.

Use the information from the planning forms or Upgrade Worksheets to complete the Software/Firmware fields.

Upgrading an existing G700 without an S8300 using the Upgrade Tool

Use the following guidelines to setup the upgrade:

- If the customer uses a common logon ID and password for multiple gateways, complete the **Common G350/G700 Logon Values** fields.
- If the customer has a centralized TFTP server for use by multiple G700 or G350 Media Gateways or the customer has a centralized FTP server for use by multiple G350 Media Gateways, complete the **Common TFTP/FTP Server Values** fields.
- Use the **Max Sessions** field to specify how many gateways can be simultaneously connected to a TFTP or a FTP server for upgrading. The number must be between one and 20 inclusive. If you do not specify a number, the Upgrade Tool defaults to six.
- If any gateways require unique logon values or unique TFTP servers, complete the **Override Common Values for G350 and G700 Targets** fields. You can enter override values for the following:
 - The IP address of the unique TFTP server.
 - The completed path to the directory from the root of the TFTP server.
 - The logon information for the gateway.
- If any override fields are left blank, the values entered in the Common fields are used.
- Some upgrades may time out due to network traffic and limitations on how long the Upgrade Tool will allow an upgrade to continue.
- Since the media gateway (MGP) firmware files are fairly large they may cause a timeout during an upgrade to a remote location. What you enter in the TFTP Directory field depends on the type of TFTP server you are using. If the TFTP server is:
 - An S8300 or an LSP, enter the path to the firmware files relative to the /tftpboot directory. For example, if the firmware files are in /tftpboot/cm4.0/728.0, enter **cm4.0/728.0**.

Note:

If the files are in the /tftpboot directory on the S8300 server/LSP and there is no subdirectory, leave the TFTP Directory field blank.

- An Avaya Windows server, enter the path of the outbound source for the TFTP server specified to be accessed. For example, if the firmware files reside in the directory `c:\ftp_outbound\cm4.0\728.3` and the TFTP server application is configured to have its outbound source as `c:\ftp_outbound`, then you would enter **cm4.0\728.3** as the value in the TFTP Directory field.

Note:

If the files are in /tftpboot on the Avaya server and there is no subdirectory, leave the TFTP Directory field blank.

- A customer server, ask the customer how their TFTP server is set up.

Note:

A TFTP server must be accessible over the LAN from the gateway you are upgrading.

3. Click **Schedule** to set up the upgrade schedule or **Run Now** to run the upgrades immediately.

Ensuring the MGP default gateway IP address is set

Communication Manager release 4.0 *requires* that the built-in VoIP module of the G700 Media Gateway has a default gateway IP address. To ensure that this IP address is set, perform the following steps:

1. Log into the G700 Media Gateway console port (see [Logging in to the P330 Stack Processor with a Direct Serial Connection](#) on page 64).
2. Type `configure` to obtain the **P330-1(configure)#** prompt.
3. At the **P330-1(configure)#** prompt, type `session mgp`.
4. At the **MG-???-1(configure)#** prompt, type `show ip route mgp`.

The list of mgp routes appears.

```
MG-001-1(super)# show ip route mgp
```

DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	135.9.80.254	motfec0	(3/0/165)
135.9.80.0	255.255.255.0	135.9.80.88	motfec0	(101/0/0)

```
MG-001-1(super)#
```

5. Check that a Gateway IP address exists for Destination 0.0.0.0.
6. If a Gateway IP address does not exist, type, at the **MG-???-1(configure)#** prompt, `set ip route 0.0.0.0 0.0.0.0 <IP_address>`, where `<IP_address>` is the default gateway IP address.

After you reboot the media gateway, the IP address is active and available.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 Stack Processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 Stack Processor.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330 Stack Processors now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330T User's Guide* (available at <http://www.avaya.com/support>).

This completes the G700 firmware upgrade procedures.

Chapter 7: Telephones and adjunct systems

This section provides information on connecting telephones and other adjunct systems. To install and wire telephones and connect their power supplies, follow the instructions in

- [Installation and wiring of telephones and power supplies](#) on page 316
- [Complete the telephone installation process](#) on page 340

In addition, you may need to install one or more adjunct systems or devices. Follow the instructions in:

- [IA 770 INTUITY AUDIX messaging application](#) on page 342
- [INTUITY AUDIX LX messaging system](#) on page 344
- [ASAI co-resident DEFINITY LAN gateway \(DLG\)](#) on page 344
- [Call center](#) on page 346
- [Avaya Integrated Management](#) on page 349
- [Uninterruptible power supply \(UPS\)](#) on page 354
- [Terminal server installation](#) on page 356
- [Call detail recording \(CDR\)](#) on page 370
- [Reliable Data Transport Tool \(RD TT\) package](#) on page 374
- [Printers](#) on page 375
- [DS1/T1 CPE loopback jack](#) on page 376
- [External modems](#) on page 391
- [Busy tone disconnect equipment for non-U.S. installations](#) on page 393
- [Music-on-hold](#) on page 394
- [Paging and announcement equipment](#) on page 398
- [Adjunct Information Sources](#) on page 399

For these adjunct systems, consult the documentation specific to the system for complete installation instructions.

Your planning documentation specifies the equipment you will be installing.



WARNING:

To reduce the risk of fire, use only 26 AWG or larger telecommunication line cords when installing telephones or adjuncts.

Installation and wiring of telephones and power supplies

The wiring procedures are the same for most Avaya telephones and other equipment.

This section provides wiring examples of similar installation procedures. These are examples only; actual wiring procedures may vary at each site. For a complete description of wiring procedures, refer to "Installing and Wiring Telephones" in *Installing the Avaya S8700 Media Server with the Avaya MCC1 or the Avaya SCC1 Media Gateway*.

After installing the hardware, dial plans, trunks, and other telephone features must be administered. These procedures are provided in the *Administrator Guide for Avaya Communication Manager*, 03-300509.

These references are on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

About connectable telephones and consoles

[Table 15: Connectable Telephone and Consoles](#) lists the telephones and consoles supported by the Avaya S8300 Media Server in a G700 Media Gateway (consult: <http://support.avaya.com>).

Table 15: Connectable Telephone and Consoles

Telephone and Console Models	Type
46xx series: ¹ 4601, 4602, 4606, 4610SW, 4612, 4620, 4620SW, 4624, 4690	Internet Protocol (IP)
96xx series: 9610, 9620, 9630, 9640, 9650	Internet Protocol (IP) ²
2410, 2420	Digital
64xx series: 6402, 6402D, 6408D+, 6416D+M, 6424D+M	Digital
603F Avaya Callmaster IV	Digital
607A Avaya Callmaster V ACD Console	Digital
606A Avaya CallMaster VI ACD Console	Digital
Enhanced Attendant Consoles: 302D	Digital

1 of 2

Table 15: Connectable Telephone and Consoles (continued)

Telephone and Console Models	Type
62xx series: 6211, 6219	Analog
2500, 2554	Analog
9040 Avaya TransTalk	Wireless
3127 Avaya Soundstation/SoundPoint Speakerphones: 3127-ATR, -STD, -EXP, -APE, -APX, -MIC, -PMI	Analog
3127 Avaya Soundstation/SoundPoint Speakerphones: 3127-DCP, -DCS, -DCE, -DPE, -DPX, -DDP, -DDX, -MIC, -PMI	Digital

2 of 2

1. For information on administering 46xx series IP Telephones, see *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507.
2. To use G.722 codec, g.722 must be supported on both ends of a call. Otherwise the 96xx telephone uses a different codec supported by the endpoints.

Connecting telephones

Various analog, digital, and IP telephones can be connected to the G700 Media Gateway. In addition, you may need to install an 808A Emergency Transfer Panel. Examples of these procedures follow:

- [Connecting an analog station or 2-wire digital station](#)
- [Installing an 808A Emergency Transfer Panel and associated telephones](#)

Connecting an analog station or 2-wire digital station

This example is typical of the 2-wire digital stations (2420, 64xx, 302D), 2-wire analog stations (2500), analog Central Office (CO) trunks, Direct Inward Dial (DID) trunks, and external alarms.

To connect an analog or 2-wire digital station

1. Choose a peripheral to connect (such as a 2-wire digital station).
2. Choose the media module to use and its media gateway and slot number; for example, MM711 Analog Media Module, Media Gateway 002, Slot V2.
3. Choose a port circuit on the MM711 Media Module; for example, port 03.

4. Install cross-connect jumpers to connect the pins from the 2-wire digital station to the appropriate pins on the MM711 Media Module. [Table 16](#) shows a pinout chart for two-wire stations.

Table 16: Two-Wire Station Pinout Chart

Jack Name	1	2	3	4	5	6	7	8
BRI-T			+TX	+RX	-RX	-TX	-V	GND
ADJUNCT	+Vadj	T0	-V	GNDVoice	RRVoice	+V	S0	TTVoice
DSS (QUEST)	DTX		DRX			OKdig	-V	+V
DSS (ISDN)								
BRI-A			GND	TX	RX	-V		
BRI-U				TX	RX		-V	GND
DCP	TX1	TX2	RX1			RX2	-V	+V
ANALOG				TIP	RING			
HANDSET			-TX	+RX	-RX	+TX		

5. Administer using *Administrator Guide for Avaya Communication Manager*, 03-300509.

Figure 21: 2500-Type Analog Telephone Wiring

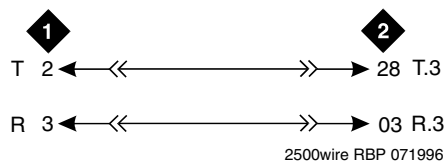


Figure notes:

1. 2500-Type Analog Station
2. MM711 Analog Media Module, Position 1V301

Connecting an ISDN BRI station to an MM720 Media Module

Each ISDN port on the MM720 Media Module (see [Media modules](#) on page 71) supports up to two ISDN BRI stations.

Note:

The MM720 BRI Media Module cannot be administered to support both BRI trunks and BRI stations at the same time. Also, the MM720 BRI Media Module does *not* support combining both B-channels together to form a 128-kbps channel. Finally, if the MM720 BRI Media Module is administered to support BRI stations, it cannot be used as a clock synchronization source.

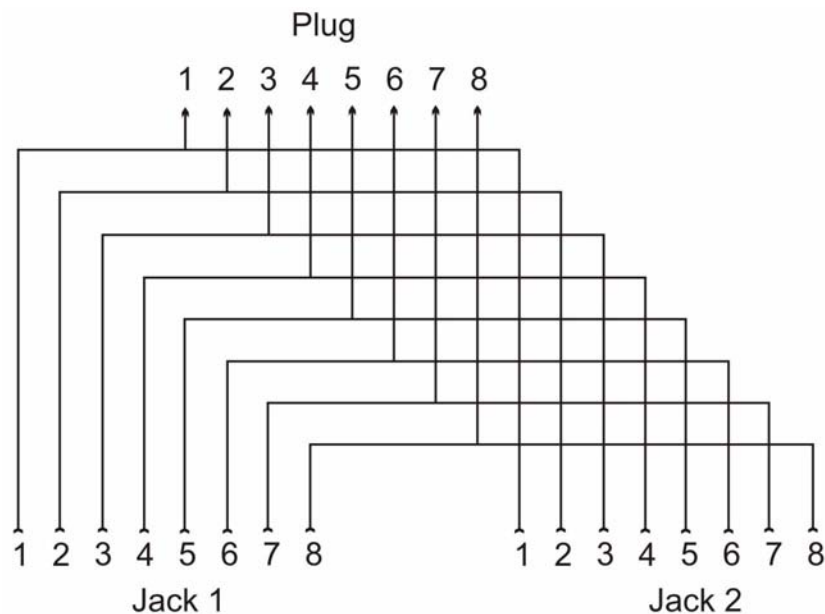
To connect one ISDN BRI station to one ISDN port:

1. Connect the station via a standard 8-pin BRI cable to one of the ISDN ports on an MM720 Media Module.

To connect two ISDN BRI stations to one ISDN port:

1. Connect each station to an RJ-45 splitter that provides two RJ-45 4-pair jacks, and one RJ-45 male connector. See [Figure 22](#) for the correct wiring for the splitter.
2. Connect the male connector of the splitter to one of the ISDN ports on an MM720 Media Module.

Figure 22: RJ-45 splitter wiring for connecting two ISDN BRI stations to one ISDN port



Installing an 808A Emergency Transfer Panel and associated telephones

Note:

Install only 1 emergency transfer power panel per system.

Emergency transfer capability is provided by an 808A Emergency Transfer Panel (or equivalent) mounted next to the trunk/auxiliary field. See [Figure 23: 808A Emergency Transfer Panel](#) on page 320.

Use analog telephones for emergency transfer. The 2500-type telephones can also be used as normal extensions. Emergency transfer capability may be provided on analog **CO** and Wide Area Telecommunications Service (**WATS**) trunks.

The transfer panel provides emergency trunk bypass or power-fail transfer for up to 5 incoming **CO** trunk loops to 5 selected station sets. The 808A equipment's Ringer Equivalency Number (REN) is 1.0A.

For information on installing the 808A Emergency Transfer Panel, see *808A Emergency Transfer Panel Installation Instructions*, which ships with the Emergency Transfer Panel.

Figure 23: 808A Emergency Transfer Panel

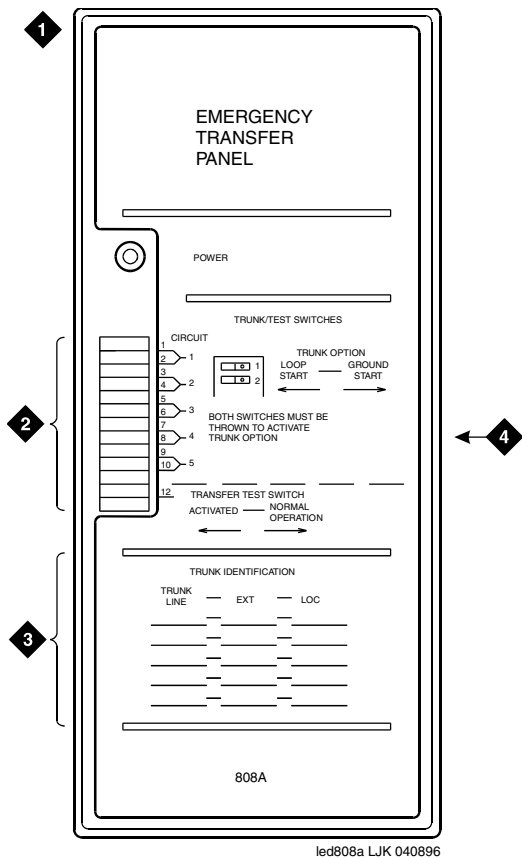


Figure notes:

1. 808A emergency transfer panel	3. Trunk identification label
2. Circuit start selection switches	4. 25-pair male connector

Installing and wiring telephone power supplies

This section provides information and wiring examples of installation procedures for various telephone and console power supplies. These are examples only and actual wiring procedures may vary at each site.

The power is provided to telephones or consoles either centrally or locally.

Centrally located power supplies include:

- [1152A1 mid-span power distribution units](#) on page 324

Local power supplies include:

- [1151B1/C1 and 1151B2/C2 power supplies](#) on page 333

Typical adjunct power connections

The 400B2 adapter is convenient for connecting local -48 VDC power to a modular plug. See [Figure 24: 400B2 Adapter Connecting to a Modular Plug](#) on page 322.

Each port network can provide power for up to three attendant consoles. This source of power is preferred for the attendant consoles because it has the same battery backup as the G700 Media Gateway.

Adjunct power can be provided locally at the telephone or console by either the 1151B1/C1 or 1151B2/C2 power supply. The 1151A1 is a standard (no battery backup) power supply unit. The 1151B2/C2 is a battery backup version of the 1151B2/C2. Either power supply can support one telephone with or without an adjunct. The maximum loop range is 250 feet (76 meters). Two modular jacks are used. Power is provided on the PHONE jack, pins 7 and 8 (- and +, respectively). Adjunct power can be provided from the equipment room or equipment closet with the 1145B power unit.

Refer to *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151, for detailed power supply information and installation procedures.

Figure 24: 400B2 Adapter Connecting to a Modular Plug

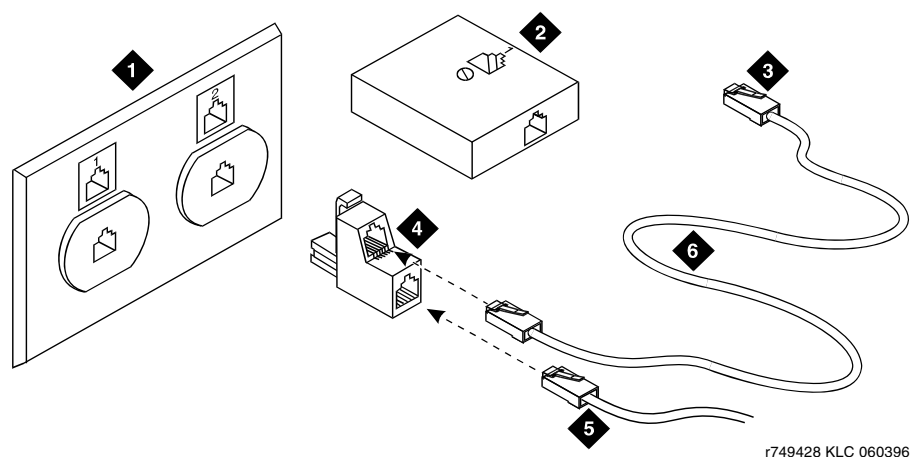


Figure notes:

1. Flush-Mounted Information Outlet	4. 400B2 Adapter
2. Surface-Mounted Information Outlet	5. To Telephone
3. To Individual Power Unit	6. Destination Service Access Point (DSAP) Power Cord

Typical adjunct power connections end-to-end

[Figure 25: Example Adjunct Power Connections](#) on page 323 shows typical connection locations for adjunct power.

Figure 25: Example Adjunct Power Connections

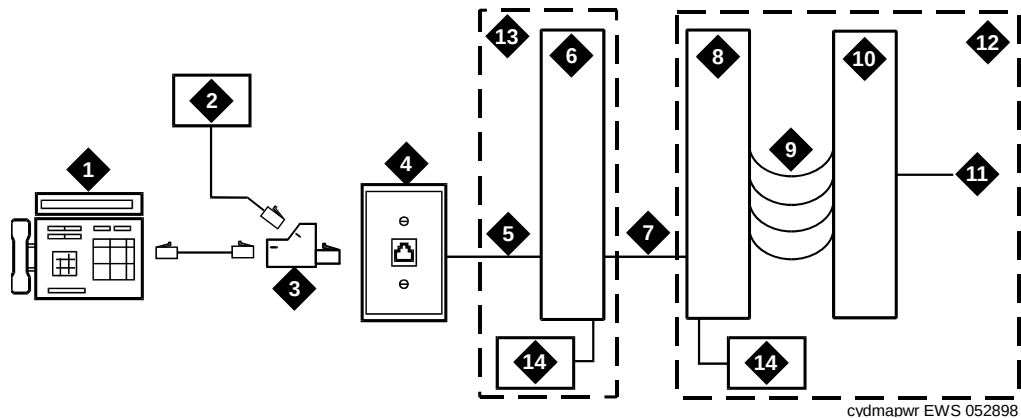


Figure notes:

1. Typical display telephone	9. 100P6A patch cord or jumpers
2. Individual power supply (Such as 1151B/C) (Not used if item 14 is used)	10. System side of MDF
3. 400B2 adapter	11. 25-pair cable to digital line modular jack
4. Information outlet (modular jack)	12. Equipment room
5. 4-pair D-Inside Wire (DIW) cable	13. Satellite location
6. Satellite site or adapter location	14. Bulk power supply. Install at satellite location or equipment room (not both).
7. 25-pair D-Inside Wire (DIW) cable	
8. Station side of MDF	

Auxiliary power for an attendant console

The nonessential functions of an attendant console and its optional 26A1 or 24A1 selector console derive power from an auxiliary power source. Provide auxiliary power for an attendant console through this cable so the console remains fully operational during short power outages.

Note:

Only 1 console can derive auxiliary power from the system and through the auxiliary cable located in the trunk/auxiliary field.

A console's maximum distance from its auxiliary power source is:

- 800 feet (244 m) for a 302A1
- 350 feet (107 m) for a 301B1 and 302D

An attendant console can also derive auxiliary power from:

- Individual 1151B/C or 1151B2/C2 power supply
- MSP-1 power supply
- 258A-type adapters
- Bulk power supplies

Local and Phantom Power

An attendant console's maximum distance from the system is limited. See [Table 17: Attendant Console Cabling Distances](#) on page 324.

Table 17: Attendant Console Cabling Distances

Enhanced Attendant Console (302D)	24 AWG Wire (0.26 mm ²)		26 AWG Wire (0.14 mm ²)	
	Feet	Meters	Feet	Meters
With Selector Console				
Phantom powered	800	244	500	152
Locally powered	5000	1524	3400	1037
Without Selector Console				
Phantom powered	1400	427	900	274
Locally powered	5000	1524	3400	1037

1152A1 mid-span power distribution units

The 1152A1 Mid-Span Power Distribution Units (PDUs) are a series of Ethernet power supplies that provide power to up to 24 46xx-series IP telephones or wireless LAN (WLAN) access points. The 1152A 1 PDUs are available in 6-port, 12-port, or 24-port sizes, with or without support for SNMP. These units are used with a 10/100BaseTx standard Ethernet network over a standard TIA/EIA-568 Category 5, 6 or 6e cabling plant. The 1152A1s meet the current requirements of the IEEE802.3af standard for resistive detection.

The 1152A1 PDU complies with the Underwriters Laboratories Inc. (UL) standard UL 1950, second edition.

Table 18: 1152A1 PDU UL 1950 Compliance

Complies	UL 1950
Approved	CSA C22.2 No.950 Std.
Approved	CE Regulatory Compliance
Approved	EN 60950
Approved	TUV EN 60950

For safety instructions, see [Important 1152A1 PDU Safety Instructions](#) on page 325. For installation instructions, see [Connecting the 1152A1 PDU cables](#) on page 326.

Important 1152A1 PDU Safety Instructions

Please read the following helpful tips. Retain these tips for later use.

When using this switch, the following safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons:

- Read and understand all instructions.
- Follow all warnings and instructions marked on this switch.
- This product can be hazardous if immersed in water. To avoid the possibility of electrical shock, do not use it near water.
- The 1152A1 PDU contains components sensitive to electrostatic discharge. Do not touch the circuit boards unless instructed to do so.
- This product should be operated only from the type of AC (and optional DC) power source indicated on the label. If you are not sure of the type of AC power being provided, contact a qualified service person.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
- Do not overload wall outlets and extension cords as this can result in the risk of line or electric shock.
- Disconnect the cords on this product and refer servicing to qualified service personnel under the following conditions:
 - The power supply cord or plug is damaged or frayed
 - Liquid has been spilled into it
 - Exposed to rain or water
 - Dropped or the housing has been damaged
 - Exhibits a distinct change in performance
 - Operates abnormally when following the operating instructions

Using the 1152A1 PDU

The 1152A1 PDU is used to power the 46xx series of IP telephones in addition to providing 10/100 megabits per second Ethernet connection.

Generation 1 Avaya IP telephones can receive power from the 1152A1 using an in-line adapter. This adapter provides the resistive signature so that the 1152A1 allows power to flow to the telephone. The generation 2 telephones do not need an adapter.

The 1152A1 PDU has 6, 12, or 24 10/100 Base-T ports, and each can supply up to 16.8 watts using the internal power supply and operates on a 100-240 volts AC, 60/50 hertz power source.

The 1152A1 PDU is 1U high and fits in most standard 19-inch racks. It can also be mounted on a shelf. Refer to the user's guide that comes with the unit for complete installation instructions.

To connect the 1152A1 PDU

CAUTION:

The 1152A1 PDU has no ON/OFF switch. To connect or disconnect power to the 1152A1 PDU, simply insert or remove the power cable from the AC power receptacle on the rear of the 1152A1 PDU.

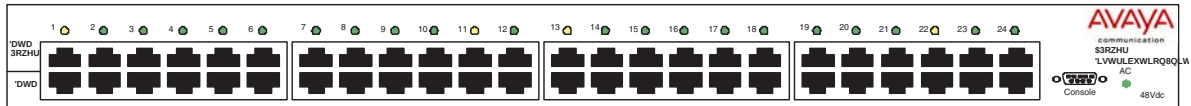
1. Plug a power cord into the power socket on the rear of the 1152A1 Power Distribution Unit.
2. Plug the other end of the power cord into the power receptacle.

The 1152A1 PDU powers up, and the internal fans begin operating.

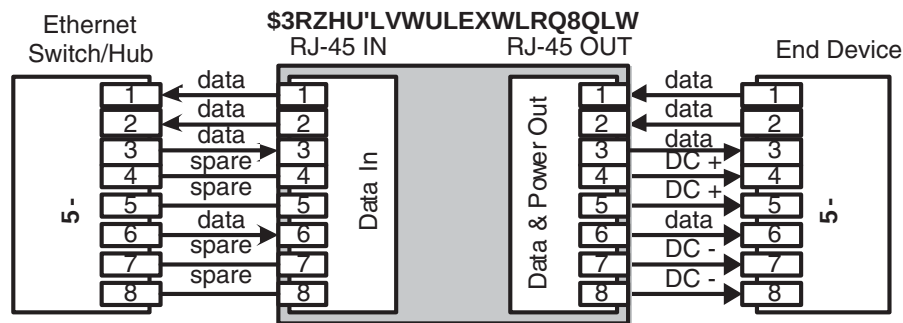
The 1152A1 PDU then runs through its Power On Self Test (POST), which takes less than 10 seconds. During the test, all the ports on the unit are disabled and the LEDs light up. For more information on the test, refer to the user's guide that comes with the unit.

Connecting the 1152A1 PDU cables

All of the ports on the front of the 1152A1 PDU are configured as data route-through ports for all data wires (pins 1, 2, 3 and 6).



Use a standard CAT5, CAT6 or CAT6e straight-through Ethernet cable (not supplied), including all 8 wires (4 pairs) as shown in [Connecting cables to telephones and other end devices](#) on page 327.

Figure 26: Connecting telephones and other end devices to the 1152A1 PDU

For Data-In ports connect the Ethernet cable leading from the Ethernet Switch/Hub to the Data port. For Data & Power Out ports connect the Ethernet cable leading to the telephone or other end device to the corresponding Data & Power port.

Note:

Be certain to connect correspondingly numbered Data and Data & Power ports.

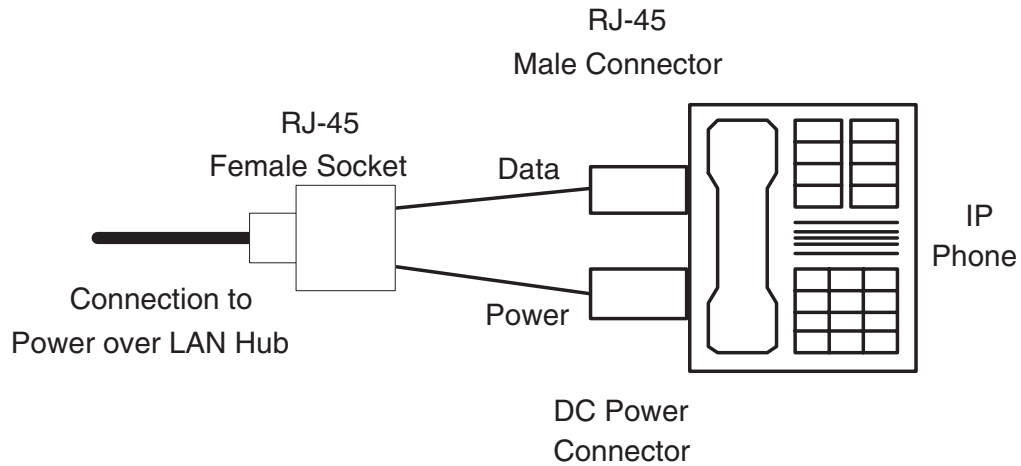
Connecting cables to telephones and other end devices

The 1152A1 PDU contains line-sensing capabilities that enable it to send power only to end devices designed to receive power from the LAN. These end devices, termed Power over LAN Enabled, receive power once they are connected to the 1152A1 PDU.

To safeguard devices that are not enabled, the 1152A1 PDU detects devices that are not enabled so does not send power. Note that data continues to flow using the Ethernet cable regardless of the status of the end device.

End devices that are not enabled to receive power directly may receive power and data through an external splitter. The external splitter separates the power and data prior to connection to the end device (see [Figure 27: Connecting an IP telephone with an external splitter](#) on page 328).

Figure 27: Connecting an IP telephone with an external splitter



Before connecting telephones or other end devices to the 1152A1 PDU, determine if the device:

- Is Power over LAN Enabled or not.

If not, you may safely connect the telephone; however, the port supplies no power and functions as a normal Ethernet data port.

- Requires an external splitter or whether it requires only a single RJ45 connection.

If an external splitter is needed, be certain to use a splitter with the correct connector and polarity.

- Power requirements are consistent with the 1152A1 PDU voltage and power ratings.

Refer to Appendix B in the user's guide that comes with the unit for voltage and power ratings.

To connect telephones and other end devices to the 1152A1 PDU

1. Connect an Ethernet cable to the telephone using an external splitter or directly (if the device is Power over LAN Enabled).
2. Connect the opposite end of the same cable to the RJ45 wall outlet.
3. On the front panel of the 1152A1 PDU, monitor the response of the corresponding port LED.
If it lights up GREEN, the unit has identified your telephone as a Power over LAN telephone.

1152B mid-span power distribution units

The Avaya 1152B Midspan Power Distribution Units are Ethernet power supplies that provide power to up to 48 46xx-series or 96xx IP telephones or wireless LAN (WLAN) access points. The 1152B PDUs are designed to deliver power in addition to data communication over an Ethernet network. The 1152B PDUs eliminate the need to connect each Ethernet Data Terminal, such as an IP Telephone set, to an AC power outlet in addition to the data port. The system also removes the need for power cables, local AC wall adapters and the use of a dedicated UPS for each IP telephone. Some models support SNMP remote management via a separate physical RJ45 input port.

These units are used with a standard 10/100BaseTx Ethernet network infrastructure using standard TIA/EIA-568 Category 5, 5e, or 6 100-Ohm Unshielded Twisted Pair (UTP) cable. The 1152B meets the current requirements of the IEEE802.3af-2003 standard for resistive detection. The 1152B PDUs also comply with Restriction of the use of Hazardous Substances (RoHS) standards.

The units are as follows:

Table 19: 1152B Midspan Power Distribution Units

Avaya Model Number	Number of Ports	SNMP	Summary
1152B48S	48	Yes	48-port, AC Input, 48Vdc Output with SNMP
1152B24S	24	Yes	24-port, AC Input, 48Vdc Output with SNMP
1152B06	6	No	6-port, AC Input, 48Vdc Output
1152B06S	6	Yes	6-port, AC Input, 48Vdc Output with SNMP

The 1152B PDU complies with the Underwriters Laboratories Inc. (UL) standard UL 60950-1, 1st Edition.

Table 20: 1152B PDU UL 60950-1 Compliance

Complies	UL 60950-1
Approved	CAN/CSA-C22.2 No. 60950-1-03Std.
Approved	CE Regulatory Compliance
Approved	EN 60950
Approved	TUV EN 60950

Important 1152B PDU Safety Instructions

Please read the following helpful tips. Retain these tips for later use.

When using this switch, the following safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons:

- Read and understand all instructions.
- Follow all warnings and instructions marked on this switch.
- This product can be hazardous if immersed in water. To avoid the possibility of electrical shock, do not use it near water.
- The 1152B PDU contains components sensitive to electrostatic discharge. Do not touch the circuit boards unless instructed to do so.
- This product should be operated only from the type of AC (and optional DC) power source indicated on the label. If you are not sure of the type of AC power being provided, contact a qualified service person.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
- Do not overload wall outlets and extension cords as this can result in the risk of line or electric shock.
- Disconnect the cords on this product and refer servicing to qualified service personnel under the following conditions:
 - The power supply cord or plug is damaged or frayed
 - Liquid has been spilled into it
 - Exposed to rain or water
 - Dropped or the housing has been damaged
 - Exhibits a distinct change in performance
 - Operates abnormally when following the operating instructions

Using the 1152B PDUs

The 1152B PDUs are used to power the 46xx series and 96xx series of IP telephones in addition to providing 10/100 megabits per second Ethernet connection.

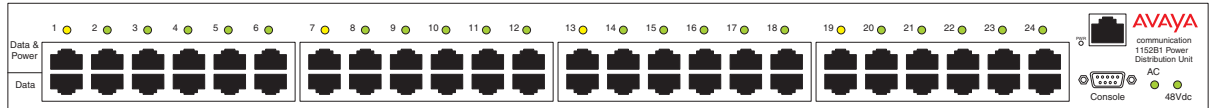
Generation 1 Avaya IP telephones can receive power from the 1152B using an in-line adapter. This adapter provides the resistive signature so that the 1152B allows power to flow to the telephone. The generation 2 telephones do not need an adapter.

The 1152B PDU has 10/100 Base-T ports, each of which can supply a minimum of 15.4 watts using the internal power supply and operates on a 100-240 volts AC, 60/50 hertz power source.

The 1152B PDU is 1U high and fits in most standard 19-inch racks. It can also be mounted on a shelf. Refer to the user's guide that comes with the unit for complete installation instructions.

Connecting the 1152B PDU cables

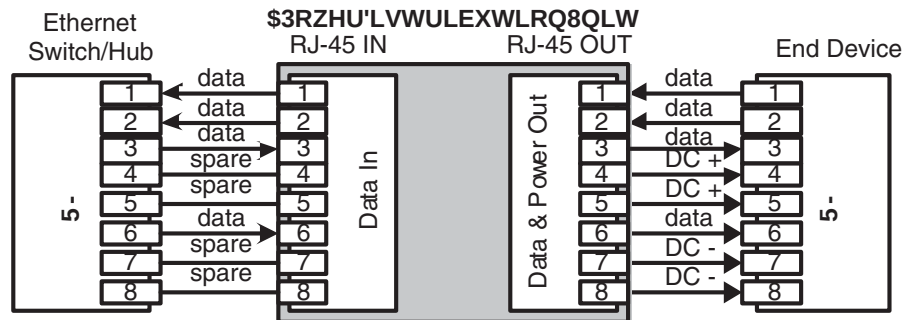
All of the ports on the front of the 1152B PDU are configured as data route-through ports for all data wires (pins 1, 2, 3 and 6).



h2cm1152 LAO 122006

Use a standard CAT5, CAT6 or CAT6e straight-through Ethernet cable (not supplied), including all 8 wires (4 pairs) as shown in [Connecting cables to telephones and other end devices](#) on page 327.

Figure 28: Connecting telephones and other end devices to the 1152B PDU



For Data-In ports connect the Ethernet cable leading from the Ethernet Switch/Hub to the Data port. For Data & Power Out ports connect the Ethernet cable leading to the telephone or other end device to the corresponding Data & Power port.

Note:

Be certain to connect correspondingly numbered Data and Data & Power ports.

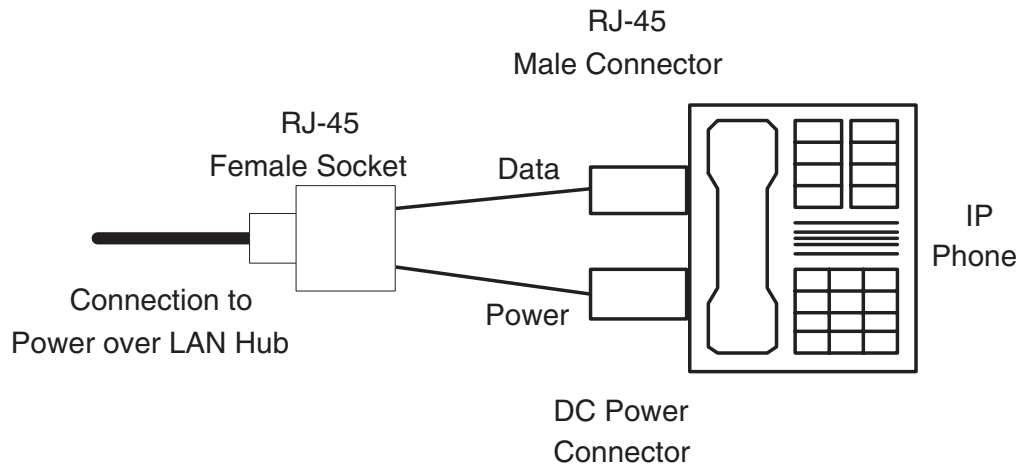
Connecting cables to telephones and other end devices

An 1152B PDU contains line-sensing capabilities that enables it to send power only to end devices designed to receive power from the LAN. These end devices, termed Power over LAN Enabled, receive power once they are connected to the 1152B PDU.

To safeguard devices that are not enabled, the 1152B PDU detects devices that are not enabled so does not send power. Note that data continues to flow using the Ethernet cable regardless of the status of the end device.

End devices that are not enabled to receive power directly may receive power and data through an external splitter. The external splitter separates the power and data prior to connection to the end device (see [Figure 29: Connecting an IP telephone with an external splitter](#) on page 332).

Figure 29: Connecting an IP telephone with an external splitter



Before connecting telephones or other end devices to the 1152B PDU, determine if the device:

- Is Power over LAN Enabled or not.

If not, you may safely connect the telephone; however, the port supplies no power and functions as a normal Ethernet data port.

- Requires an external splitter or whether it requires only a single RJ45 connection.

If an external splitter is needed, be certain to use a splitter with the correct connector and polarity.

- Power requirements are consistent with the 1152B PDU voltage and power ratings.

Refer to Appendix B in the user's guide that comes with the unit for voltage and power ratings.

To connect telephones and other end devices to the 1152B PDU

1. Connect an Ethernet cable to the telephone using an external splitter or directly (if the device is Power over LAN Enabled).
2. Connect the opposite end of the same cable to the RJ45 wall outlet.
3. On the front panel of the 1152B PDU, monitor the response of the corresponding port LED.
If it lights up GREEN, the unit has identified your telephone as a Power over LAN telephone.

1151B1/C1 and 1151B2/C2 power supplies

The 1151B1/C1 and 1151B2/C2 power supplies are local power supplies. The telephones or consoles connect directly to them through an RJ45 connector. The 1151B2/C2 has a battery backup.

These power supplies comply with the Underwriters Laboratories Inc. (UL) Standard UL 60950 third edition.

**Table 21: 1151B1/C1 and 1151B2/C2
Power Supply UL 60950 Compliance**

Complies	UL 60950
Certified	CSA 22.2
Approved	EN6950
Approved	CE

For safety instructions, see [Important safety instructions for 1151B1/C1 and 1151B2/C2 power supplies](#) on page 334. For installation instructions, see [Connecting the 1151B1/C1 or 1151B2/C2 power supplies](#) on page 335.

Important safety instructions for 1151B1/C1 and 1151B2/C2 power supplies

Please read the following helpful tips. Retain these tips for later use.

When using this power supply, the following safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons:

- Read and understand all instructions.
- Follow all warnings and instructions marked on this power supply.
- This product can be hazardous if immersed in water. To avoid the possibility of electrical shock, do not use it near water.
- To reduce the risk of electric shock, do not disassemble this product except to replace the battery.
- This product should be operated only from the type of AC power source indicated on the label. If you are not sure of the type of AC power being provided, contact a qualified service person.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
- Do not overload wall outlets and extension cords as this can result in the risk of line or electric shock.
- Disconnect the cords on this product and refer servicing to qualified service personnel under the following conditions:
 - The power supply cord or plug is damaged or frayed
 - Liquid has been spilled into it
 - Exposed to rain or water
 - Dropped or the housing has been damaged
 - Exhibits a distinct change in performance
 - Operates abnormally when following the operating instructions

Using the 1151B1/C1 and 1151B2/C2 power supplies

The 1151B1/C1 and 1151B2/C2 Power Supplies can be used to supply local power to ISDN-T 85xx and 84xx series and 46xx series telephones connected to a media gateway and to the 302D Attendant Console that requires auxiliary power for its display. The unit can supply power to adjunct equipment such as S201A and CS201A speakerphones or a 500A Headset Adapter attached to any currently manufactured analog, **DCP**, or ISDN-T telephone equipped with an adjunct jack.



CAUTION:

The power supply can be used *only* with telecommunications equipment, indoors, and in a controlled environment.

The power supply has a single output of -48 volts DC, 0.4 amperes and can operate from either a 120 volts AC 60 hertz power source (105 to 129 volts AC) or a 220/230/240 volts AC 50 hertz power source (198 to 264 volts AC). Input voltage selection is automatic. The output capacity is 19.2 watts.

The power supply can be placed on a flat surface such as a desk. For wall-mounting, keyhole slots are provided on the bottom of the chassis.



CAUTION:

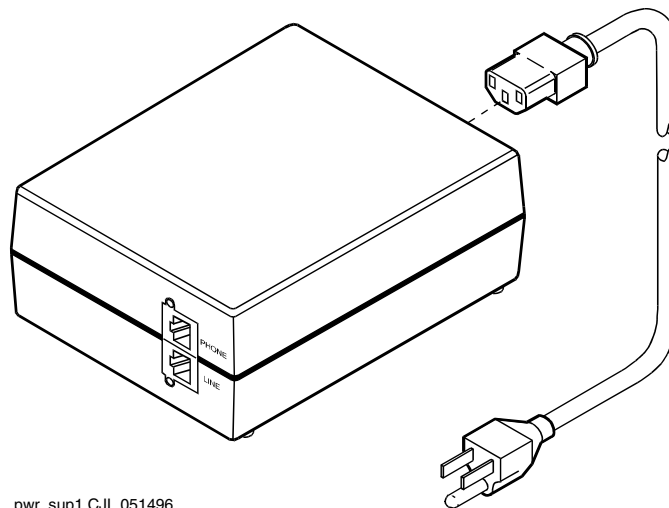
Do not locate the unit within 6 inches (15 centimeters) of the floor.

Connecting the 1151B1/C1 or 1151B2/C2 power supplies

The 1151B1/C1 is a standard (no battery backup) power supply unit. The 1151B2/C2 is a battery backup version of the 1151B1/C1. Either power supply can support one telephone with or without an adjunct. The maximum loop range is 250 feet (76 meters). Two modular jacks are used. Power is provided on the PHONE jack, pins 7 and 8 (- and +, respectively).

The PHONE and LINE jacks are 8-pin female non-keyed 657-type jacks that can accept D4, D6, and D8 modular plug cables. See [Figure 30: 1151B2/C2 Power Supply — Front](#) on page 335.

Figure 30: 1151B2/C2 Power Supply — Front



pwr_sup1 CJL 051496

C360-PWR Power over Ethernet converged stackable switches

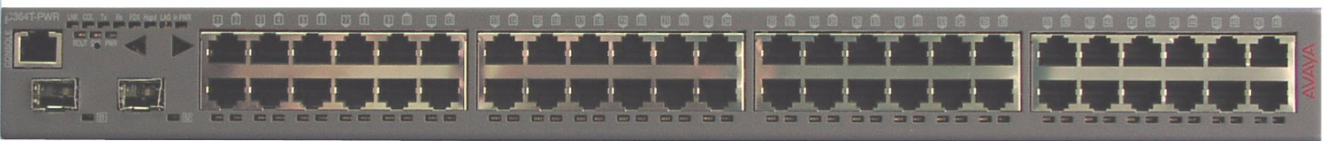
The C360T-PWR series of converged stackable switches provide a range of IEEE 802.3af Power over Ethernet (PoE) configuration options for converged networks. The C360T-PWR series switches include the C363T-PWR and the C364T-PWR switches, which provide 24 and 48 10/100 Mbps Ethernet port, respectively. Each switch also provides 2 Gigabit Ethernet ports that support SFP GBIC transceivers. Both switches are stackable and can be configured in either Layer 2 or Layer 3 switch mode.

[Figure 31](#) and [Figure 32](#) show the front panels of the C360T-PWR switches.

Figure 31: C363T_PWR front panel



Figure 32: C364T-PWR front panel



Important C360T-PWR switch safety instructions

Please read the following helpful safety tips. Retain these tips for later use.

When using this switch, the following safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons:

- Read and understand all instructions.
- Follow all warnings and instructions marked on this switch.
- This product can be hazardous if immersed in water.
To avoid the possibility of electrical shock, do not use it near water.
- The Avaya C360T-PWR switch and modules contain components sensitive to electrostatic discharge.
Do not touch the circuit boards unless instructed to do so.
- This product should be operated only from the type of AC (and optional backup DC) power source indicated on the label.

- If you are not sure of the type of AC power being provided, contact a qualified service person.
- Do not allow anything to rest on the power cord.
Do not locate this product where the cord will be abused by persons walking on it.
- Do not overload wall outlets and extension cords as this can result in the risk of line or electric shock.
- Disconnect the cords on this product and refer servicing to qualified service personnel under the following conditions:
 - The power supply cord or plug is damaged or frayed
 - Liquid has been spilled into it
 - Exposed to rain or water
 - Dropped or the housing has been damaged
 - Exhibits a distinct change in performance
 - Operates abnormally when following the operating instructions

UL safety standards compliance

The C360T-PWR complies with the Underwriters Laboratories Inc. (UL) standard UL 60950, third edition.

- UL listed to UL60950-1
- C-UL (UL for Canada) certified to CAN/CSA-C22.2 No.60950-0-03
- CE for Europe approved according to EN
- Laser components are Laser Class I approved:
 - EN-60825/IEC-825 for Europe
 - FDA CFR 1040 for USA
- Branch Circuit Protection: A UL Listed and CSA Certified 15A branch circuit protective device is to be provided in the building AC mains wiring installation.



CAUTION:

The Avaya C360T-PWR switches do not contain any user-serviceable components inside. Do not open the case.



CAUTION:

The C360T-PWR switches can be used only indoors and in a controlled environment.

Compatibility

The C360T-PWR Converged Stackable switches interoperate with any standards-based Ethernet switch and support 802.3af-compliant devices.

Power Specifications

[Table 22](#) lists the power specifications for the C360T-PWR switches.

Table 22: C360T-PWR specifications

	C363T-PWR	C364T-PWR
Input power requirements (at 100 to 240 VAC, 50–60 Hz)	305 W	520 W
Maximum power consumption	420 W	760 W
Maximum AC input current	4.2 A	7.6 A
Maximum DC input current	8 A	15 A

Using the C360T-PWR switches

The C360T-PWR Power over Ethernet Stackable Switches can be used to power 46xx-series IP and 96xx-series telephones in addition to providing a 10/100 Mbps Ethernet connection. The switches can form part of a stack with the G700 Media Gateway or members of the P33x stackable switching system. Each port on the C360T-PWR switches can supply up to 15.4 watts using the internal power supply.

The C360T-PWR switches can be placed in a wiring closet or on a flat, stable surface such as a desk. Screws are provided for mounting in a standard 19-inch rack.

Connecting the C360T-PWR switches

To power up—AC input

1. Insert the AC power cord into the AC power connector on the left side of the rear panel. See [Figure 33: C360T-PWR rear panel](#) on page 338.

Figure 33: C360T-PWR rear panel



2. Insert the other end of the power cord into a non-switched electrical AC outlet or the connector on the BUPS.

The unit powers up and performs a self-test procedure. The LEDs flash at regular intervals after the self-test procedure is completed successfully.

3. Connect the BUPS DC power supply (if applicable).

The C360T-PWR switches operate on the AC input only. However, you can use the optional DC input to:

- backup the power over Ethernet ports
- provide additional power for the Power over Ethernet ports

Note:

Please refer to the C360T-PWR switch User's Guide for more information.

Connecting the cables

To connect IP telephones, PCs, servers, routers, workstations, and hubs:

1. Connect the Ethernet connection cable (not supplied) to a 10/100 megabits per second port on the front panel of the Avaya C360T-PWR switches.

Note:

Use standard RJ45 connections and a CAT5 cable for 100 megabits per second operation.

2. Connect the other end of the cable to the Ethernet port of the PC, server, router, workstation, IP telephone, switch, or hub.

Note:

Use a crossover cable when connecting the Avaya C360T-PWR switches to a switch or hub.

3. Check that the appropriate link (LNK) LEDs light up.

Additional information

For additional information about the C360T-PWR switches, see:

Quick Start for Hardware Installation: Avaya C360 Converged Stackable Switches, 10-300616.

Installation and Configuration for the Avaya C360 Converged Stackable Switches, 10-300503.

Complete the telephone installation process

Consult the planning documentation to obtain the necessary information to complete the installation. Part of the final process involves:

- [Installing the coupled bonding conductor](#) on page 340
- [Installing over-voltage and sneak-current circuit protection](#) on page 341

Installing the coupled bonding conductor

The Coupled Bonding Conductor (CBC) provides mutual inductance coupling between the CBC and the telephone cables that are exposed to lightning. The conductor can be a 10 AWG (4 mm²) wire tie wrapped to the exposed cables, a metal cable shield around the exposed cables, or six spare pairs from the exposed cable. In a high-rise building, connect the CBC to an approved building ground on each floor.

Before you begin, be sure the telephone lines are cross-connected to the appropriate media module(s).

To install the CBC:

1. Connect one end of the conductor to a telephone cable building entrance protector ground that is connected to an approved ground.
2. Route the rest of the conductor next to the exposed telephone cables being protected until they reach the cross-connect nearest to the telephone system.
3. Terminate the other end to the single-point ground block provided for the telephone system.

Note:

Position the non-exposed telephone cables at least 12 inches (30.5 cm) away from exposed telephone cables whenever possible.

Installing over-voltage and sneak-current circuit protection

Over-voltage and sneak fuse protection measures are necessary for the safe operation of the G700 Media Gateway system. Out-of-building installations of telephones or other standard (tip/ring) devices/terminals that connect to the Avaya G700 Media Gateway Media Modules require over-voltage and sneak current protection at both building entry points. Sneak current protectors must have a maximum of 350 mA and a minimum voltage rating of 600V.

The following devices have been evaluated or tested and approved to protect the Media Modules from over-voltages and sneak current protection:

- Avaya MM712 DCP: either 146E IROB (In-Range Out-of-Building) or 4C3S-75 solid state protectors for surge and sneak current.
- Avaya MM710 T1/E1: over-voltage and sneak protection for the Avaya MM710 T1/E1 Media Module is provided on the Media Module itself.
- Avaya MM711 Analog: analog trunks use the 507B or 110-SCP-9 sneak current protectors. Over-voltage protection is normally provided by the local telephone company. Analog voice terminals use one of the following types of combined over-voltage and sneak current protection:
 - Gas tube with heat coil: 4B1E-W
 - Solid state with heat coil: 4C1S
 - IROB: 146C (4-lines) or 146F (25-lines)

**WARNING:**

Only service-trained personnel must install these circuit protection devices.

IA 770 INTUITY AUDIX messaging application

Note:

For complete information on IA 770 INTUITY AUDIX Installations, see *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532.

The IA 770 INTUITY AUDIX Messaging Application runs on a G700 Media Gateway controlled by an S8300 Media Server. Without the need for additional hardware, IA770 INTUITY AUDIX software processes touchtones, converts messages to the G.711 format, and converts text to speech.



CAUTION:

IA770 INTUITY AUDIX Messaging processes messages using the G.711 codec only. Therefore, ensure that a codec set exists that uses only the G.711 codec. Then, assign that codec set to a network region. And, finally, assign that network region to the AUDIX signaling group that is linked to the IA770 INTUITY AUDIX Messaging trunk group.

Shared resources of IA770 coresidency

An IA770 uses many resources of the S8300 Media Server and the media gateway where it resides. The following list outlines the S8300's shared resources used by the IA770 INTUITY AUDIX system:

- Hardware for data storage and retrieval
- TFTP server for:
 - Downloading and updating the license file for feature activation
 - Backing up and restoring data over a LAN or a WAN, including translations and messages
 - Updating and upgrading software
- IP address for administration access
- General Alarm Manager for alarm display
- Web interface to start and stop the system

The IA770 system also shares the same switch-tone parameters established for the S8300 Media Server. With the software-only version of the IA770 system that is currently sold, the S8300 Media Server handles switch tones on behalf of the IA770 system and passes on the control information to the IA770 system using QSIG signaling. With the IA770 system that uses a CWY1 board, the installer or administrator must set IA770 parameters to match those of the S8300 Media Server.

Where is the IA770 location and software

IA770 INTUITY AUDIX messaging is a software-only version of INTUITY AUDIX messaging that uses a QSIG-MWI H.323 virtual trunk for communication between the Communication Manager and IA770 software. The INTUITY AUDIX system software is loaded directly onto the S8300 hard drive.

Note:

For upgrades only, a G700 Media Gateway that previously used a CWY1 board can continue to use the CWY1 board with IA770 INTUITY AUDIX software. However, the CWY1 board is no longer available for new systems.

Using an AUDIX trunk group as well as an AUDIX hunt group for new systems

For new systems, an H.323 virtual trunk integration must be established. The virtual trunk group, and signaling group, setup is handled automatically when you install IA770 INTUITY AUDIX Messaging with the Avaya Installation Wizard. Otherwise, you must administer the trunk group, its signaling group, and the assigned network region and IP codec set with Communication Manager once the software is installed. The number of trunks assigned to the trunk group can be either 3, 6, or 12.

The use of trunks replaces the need for voice ports in the hunt group. However, an INTUITY AUDIX hunt group must still be defined. The hunt group setup is also handled automatically when you install IA770 INTUITY AUDIX Messaging with the Avaya Installation Wizard. Otherwise, you must administer the hunt group using Communication Manager. Other switch administration tasks that are associated with proper hunt group functions, such as creating COR, COS, and coverage paths, are also required.

IA 770 INTUITY AUDIX installations and S8300 upgrades for IA 770 INTUITY AUDIX

The INTUITY AUDIX software must be installed or upgraded at the same time as the S8300 Communication Manager software load (the **.rpm** files). The IA770 software is delivered on the Communication Manager software distribution CD. The Communication Manager installation tools install IA770 INTUITY AUDIX automatically.

For complete information on IA 770 INTUITY AUDIX Installations *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532.

INTUITY AUDIX LX messaging system

The process of integrating an INTUITY AUDIX LX system with an Avaya S8300 Media Server involves a series of tasks to prepare the switch to work with the INTUITY AUDIX LX system.

The procedures for this process are fully documented in *INTUITY AUDIX LX Release 1.0 Documentation, 585-313-818*. The information is contained in a document with the title INTUITY AUDIX LX Release 1.0 LAN Integration with S8300 and DEFINITY® Systems.

ASAI co-resident DEFINITY LAN gateway (DLG)

The DEFINITY LAN Gateway (DLG) is an application that enables communications between TCP/IP clients and Communication Manager call processing. In more technical terms, the DLG application is software that both routes Internet work messages from one protocol to another (ISDN to TCP/IP) and bridges all ASAI message traffic (by way of a TCP/IP tunnel protocol).

The DLG listens for client connections (a specific IP Address) over a well-known TCP port (5678). The client accesses the DLG's services by connecting to TCP port 5678 at the IP address of the DLG's Ethernet interface, which can be a MAPD (TN801B), a Processor (TN2314), or a C-LAN (TN799). The client then exchanges TCP Tunnel Protocol messages with the DLG to request a connection to a specific Computer Telephony Integration (CTI) link. The DLG authenticates the client based on its administration and then establishes or refuses the connection. Once a connection is established, the ASAI layer 3 messages are transparently passed through the DLG (that is, the DLG does not process any message content). Each TCP connection to the DLG has a one-to-one correspondence with a CTI link.

The DLG application is packaged either **externally** on a separate circuit pack (the TN801 MAPD circuit pack) or **internally**, where it co-resides with Communication Manager. The externally packaged DLG is referred to as the **MAPD DLG**, and the internally packaged DLG is referred to as the **Co-Resident DLG**. The Co-Resident DLG and the MAPD DLG accomplish the same basic function (ASAI to Ethernet transport).

The Co-Resident DLG is application software that co-resides with Communication Manager on the Media Server running Communication Manager. No physical installation or MAPD-specific administration is required for the Co-Resident DLG. In terms of switch-based connectivity, the Co-Resident DLG is supported by the following platforms:

- Avaya S8300 Media Server with Avaya G700 Media Gateway

Administration of the Co-Resident DLG is carried out on the switch using the **change ip-services** SAT command. When the service type DLG is specified on the **IP Services** screen, the **DLG administration** screen displays. The Co-Resident DLG does not rely on ports. Port allocation is not required for administering the Co-Resident DLG.

For Avaya S8300 Media Server with Avaya G700 Media Gateway, the Co-Resident DLG relies on the S8300 Media Server for Ethernet connectivity.

PROCR administration task summary (for the S8300 Media Server)

To administer PROCR on the S8300 Media Server with G700 Media Gateway:

1. On the SAT interface, type `display system-parameters customer-options`.

Go to page 4 and make sure that **Processor Ethernet** is enabled.

2. Type `display ip-interfaces`

Make sure the PROCR is administered and its **Ethernet port** is enabled. If the PROCR is not listed (PROCR should appear in the **Type** option field), add the PROCR.

To administer CTI links:

1. Use the `display system-parameters customer-options` command and make sure the following option is set to `yes`:

`Co-Res DEFINITY LAN GATEWAY (y)`

2. Use the `add cti-link` command to administer a CTI link.

3. Use the `change ip-services` command and specify a **Service Type** of **DLG**.

When **Service Type DLG** is entered, the system adds a **DLG Administration** page as the last of the form.

4. Complete the **DLG Administration** page to add your client information.

Note:

A CTI link must be administered before a link number can be entered. For more information and detailed procedures, refer to *CallVisor® ASAI Technical Reference*, 555-230-220.

Supported Ethernet Interfaces

[Table 23: Ethernet Interfaces](#) summarizes Ethernet interfaces used by several current switching platforms:

Table 23: Ethernet Interfaces

Platform	Processor Ethernet Interface?	C-LAN (TN799) Ethernet Interface
DEFINITY Servers csi, si, and r	No	Yes
Avaya S8100 Media Server (formerly DEFINITY ONE/ IP600)	Yes	Yes
Avaya S8300 Media Server with Avaya G700 Media Gateway	Yes	No

Call center

The S8300 Media Server provides a excellent solution for a small call center. The S8300 Media Server with the G700 Media Gateway supports the following call center capabilities:

- All three Avaya call center packages:
 - Avaya Call Center Basic
 - Avaya Call Center Deluxe
 - Avaya Call Center Elite
- Up to 450 agents
- A maximum of 16 ASAI links
- Avaya G700 announcement software

About Avaya G700 announcement software

Voice announcements are used in a call center environment to announce delays, direct customers to different departments, and entertain and inform calling parties. The announcement capability is standard and comes co-resident on the G700. The G700 announcement software has many of the functions of the TN2501AP VAL circuit pack.

See [Table 24: Comparison between the G700 Announcement software and the VAL circuit pack](#) on page 347 for differences between the Avaya G700 Announcement software and the VAL circuit pack. For more information on Avaya G700 Announcement software, see the *Administrator Guide for Avaya Communication Manager*, 03-300509, Chapter 13, "Managing Announcements".

Table 24: Comparison between the G700 Announcement software and the VAL circuit pack

Area description	TN2501AP (VAL) circuit pack	Avaya G700 announcement software
Requires hardware	Yes	No
Maximum storage time per board for TN750 or TN2501AP	Up to 60 minutes at 64 Kbps sample rate	Up to 20 minutes at 64Kbps uncompressed speech
Concurrent Calls per Announcement	50 when using a DEFINITY Server SI or DEFINITY Server CSI 1,000 when using the DEFINITY Server R, S8500, or S8700/S8710 Media Server	1,000
Backup and restore over LAN	Yes	Yes
Recording Method	Use PC or telephone	Use PC or telephone
File portability to multiple DEFINITY or Communication Manager servers	Yes	Yes

1 of 2

**Table 24: Comparison between the G700
Announcement software and the VAL circuit pack (continued)**

Area description	TN2501AP (VAL) circuit pack	Avaya G700 announcement software
Playback quality	Toll quality	Toll quality
Backup speed	2.6 seconds for each 60 seconds of announcement time	2.6 seconds for each 60 seconds of announcement time
Reliability	High	High
Firmware downloadable	Yes	Yes
Number of boards per system	5 on the DEFINITY CSI and DEFINITY SI 10 on the DEFINITY R and S8500 or S8700/S8710 Media Server	10 per configuration
Announcements per board	256	256
Maximum number of announcements in a configuration	128 DEFINITY Server CSI or DEFINITY Server Si 1,000 DEFINITY Server R 3,000 S8500, or S8700/S8710 Media Server	3,000 over multiple G700 Media Gateways
Format	CCITT A-law or u-law	CCITT A-law or u-law
Sample bits	8	8
Sample rate	8,000 KHz	8,000 KHz
Channels	Mono	Mono

2 of 2

Avaya Integrated Management

Avaya Integrated Management provides a comprehensive set of network and system management solutions for the converged voice and data environment. Avaya Integrated Management is available in several different offers. Each offer includes an appropriate set of applications to meet different business needs. Contact your client executive to learn which offer best meets the needs of your enterprise.

Avaya Integrated Management architecture provides standards-based infrastructure for integrated management applications. The individual applications over time will become integrated with a common look and feel. The available products include:

- [Avaya ATM WAN Survivable Processor Manager](#)
- [Avaya Directory Enabled Management](#)
- [Avaya Network Management Console with VoIP SystemView](#)
- [Avaya MultiService SMON Manager](#)
- [Avaya Fault and Performance Manager](#)
- [Avaya Proxy Agent](#)
- [Avaya Configuration Manager](#)
- [Avaya Site Administration](#)
- [Avaya Terminal Configuration](#)
- [Avaya Terminal Emulator](#)
- [Avaya Voice Announcement Over LAN Manager](#)
- [Avaya VoIP Monitoring Manager](#)

Avaya ATM WAN Survivable Processor Manager

Avaya ATM WAN Survivable Processor Manager is a Windows (98/NT/2000) client/server software tool with which administrators can upload translations from a main Media Server to the Avaya ATM WAN Survivable Processor Manager workstation. Once translations are uploaded, administrators can then download them from the workstation to a maximum of 15 separate ATM WSP Media Servers using LAN connectivity.

Avaya Directory Enabled Management

Avaya Directory Enabled Management is a web-based software solution that provides real-time Directory-based (LDAP) read/write access to Media Servers. Avaya Directory Enabled Management provides the capability to keep data, such as station and subscriber data, synchronized with its image in the LDAP data store, and provides a rules engine that facilitates the management of these servers/applications, based on events (add/delete/modify) that take place at servers or applications. Currently, Avaya Directory Enabled Management operates only with Microsoft Internet Explorer.

Avaya Network Management Console with VoIP SystemView

Avaya Network Management Console with VoIP SystemView provides customers with either a standalone product or one that can integrate with the HP OpenView NMS, and includes applications that allow customers to manage network devices. These applications include:

- Avaya MultiService Address Manager — displays a centralized list of hosts in the network, and correlates among IP addresses, MAC addresses, and device port connectivity.
- Avaya MultiService Configuration Manager — provides quick network setup and installation, fast recovery for faulty devices, downloading/uploading configuration data, backup of configuration files, and export of configuration files to other sources for reporting or analysis.

Accessible from within Avaya MultiService Configuration Manager, Avaya MultiService EZ2Rule Manager is a campus-wide application that provides Quality of Service (QoS) management for small sites with limited bandwidth resources. In addition, Avaya MultiService EZ2Rule Manager enables the user to preview the application of new rules before network deployment, ensuring accurate and consistent deployment of priorities in the network.

- Avaya MultiService Console — provides the discovery of IP-enabled devices, hierarchical map representation, device status, fault monitoring, and a launch point for device managers.
- Avaya MultiService Software Update Manager — downloads software to managed Avaya MultiService devices, and performs all necessary software maintenance operations. These operations include checking current software versions against the latest versions available from the Avaya Web site, recommending service packs, and providing an inventory of Avaya MultiService data devices residing on the network.
- Avaya MultiService VLAN Manager — a graphical application for VLAN management that allows for configuration and monitoring of VLAN use. Avaya MultiService VLAN Manager assigns and maintains VLAN numbering and naming, tracks additions and changes to the network, validates VLAN name and tag values, and monitors the number of VLANs in order to assist in maintenance tasks.

Avaya Network Management Console with VoIP SystemView supports converged network environments composed of multi-vendor equipment from key vendors and will be enhanced to support all Avaya IP voice systems and data devices to create a full convergence solution.

Avaya MultiService SMON Manager

Avaya MultiService SMON Manager monitors the Ethernet and provides complete visibility of all switched traffic in the network. Although SMON Manager is an application provided with Avaya Network Management Console with VoIP SystemView, SMON Manager requires a license key before it can be used.

Avaya Fault and Performance Manager

Avaya Fault and Performance Manager operates standalone or with Avaya Network Management Console with VoIP SystemView and/or HP OpenView to provide a network map or system view of a converged network. Use it to view fault and performance data, busyout boards and ports, acknowledge exceptions, and configure collection times and information.

Avaya Proxy Agent

Avaya Proxy Agent is the SNMP proxy agent that provides an interface to Media Servers running DEFINITY Release 9 software through and including current versions of Avaya Communication Manager. Avaya Proxy Agent provides a protocol conversion between the proprietary OSSI protocol and SNMP.

Avaya Configuration Manager

Avaya Configuration Manager allows you to administer Media Servers running DEFINITY Release 9 software through and including Avaya current versions of Avaya Communication Manager. Multiple administrators can access multiple Media Servers. Administrators can perform station moves/adds/changes, print button labels, as well as many other common administrative activities. Avaya Configuration Manager provides a web-based Graphical User Interface (GUI) client that runs in the supported browsers and allows administrators access Communication Manager from any workstation on the network.

Avaya Site Administration

Avaya Site Administration is a PC-based Windows (98/NT/2000) tool that lets you administer Media Servers running DEFINITY Release 9 software through and including current versions of Avaya Communication Manager, and AUDIX Messaging Systems. Avaya Site Administration simplifies administration with an easy-to-use interface that offers wizards and GEDI (Graphically Enhanced DEFINITY Interface), as well as terminal emulation.

Avaya Terminal Configuration

Avaya Terminal Configuration is a web-based client application that allows end users to access Media Servers in order to configure personal station set preferences and features. Avaya Terminal Configuration runs on top of Avaya Directory Enabled Management software, and therefore requires that Avaya Directory Enabled Management software be installed.

Avaya Terminal Emulator

Avaya Terminal Emulator is a Windows (98/NT/2000) application that provides direct connectivity capabilities. It can be run either as a standalone application or run from Avaya Site Administration. Avaya Terminal Emulator includes the following features:

Connection List — lets you store and organize information about the systems to which you regularly connect and allows you to connect to them by double-clicking.

FTP Manipulator — lets you transfer files to and from your computer to a remote system.

Icon Manager — lets you assign functionality to icons that come as part of Avaya Terminal Emulator or to your own icons.

Telnet connection — lets you launch a telnet session to remote systems that you are accessing over a LAN or WAN.

Terminal Emulator — lets you access systems using a modem, data module, PDM, or direct connection.

Avaya Voice Announcement Over LAN Manager

Avaya Voice Announcement over LAN Manager lets you use your LAN to transfer recorded announcements to the TN2501AP boards located in remote Media Servers.

Avaya Voice Announcement over LAN Manager offers the following capabilities:

- View the current status of TN2501AP board announcements
- Simplified administration to add/change/remove announcements
- Copy/backup announcement files from a supported TN2501AP board to Avaya Voice Announcement over LAN Manager using a customer's LAN
- Copy/restore announcement files to a supported TN2501AP board from Avaya Voice Announcement over LAN Manager using a customer's LAN

Avaya VoIP Monitoring Manager

Avaya VoIP Monitoring Manager is Windows 2000 application that allows you to monitor real-time Quality of Service (QoS) measurements for VoIP systems. Avaya VoIP Monitoring Manager offers a client GUI accessible from your LAN or using remote access. Avaya VoIP Monitoring Manager can generate traps associated with VoIP QoS sent to any NMS, and can receive RTCP packets from IP telephones, IP soft phones, VoIP engines (on G700 Media Gateways), and Prowler boards. Avaya VoIP Monitoring Manager can operate as a standalone application, or it can be integrated with Avaya Network Management Console with VoIP SystemView.

Uninterruptible power supply (UPS)

The Avaya 1000-2000 VA online Uninterruptible power systems (UPSs) provide power protection for telecommunications systems and equipment. Avaya UPSs are a cost-effective measure to avoid costly downtime. The Avaya UPS provides complete isolation from power disturbances to protect customer's data and equipment. It can keep the phones up and ensure network reliability, but it also provides customizable alarm and monitoring capabilities.

Avaya online UPSs feature:

- Isolation of connected equipment from all incoming power problems
- Doubled battery service life and advanced warning of the end of useful battery life with Advanced Battery Management (ABM) technology
- Prolonged backup time with Extended Battery Modules (EBMs)
- Conditioned incoming power without depleting the battery to preserve battery power for complete power outages
- Adapted to rack-mount and standalone tower applications with two-in-one form factor
- Standard RS-232 communications port
- Standard DEFINITY alarm contacts
- Six-foot communications cable included
- Web/SNMP card to add direct control and monitoring capabilities in SNMP-based networks and via Web browsers (Optional for all models except select 1000 VA UPS).

Model selection guide and specifications

Model	SAP Code	Power Out (VA/Watt)	Output Receptacles ¹	Dimensions (HxWxD) ²	Weight (lb)
UPS Models: 120 Vac³, 50/60 Hz, auto-sensing					
1000 VA w/Web/SNMP Card	700290273	700/490	(6) 5-15R	3.5 x 17.0 x 19.4 in.	34
1000 VA	408357010	1000/700	(6) 5-15R	3.5 x 17.0 x 19.4 in.	34
1500 VA	408357028	1500/1050	(6) 5-15R	3.5 x 17.0 x 19.4 in.	50
2000 VA	700019300	2000/1400	(4) 5-15R & (2) 5-20R	3.5 x 17.0 x 19.4 in.	50
Optional Extended Battery Modules (EBMs)					
EBM 24V	408357044	-	-	3.5 x 17.0 x 19.4 in.	65
EBM 48V	408357051	-	-	3.5 x 17.0 x 19.4 in.	65
XBU48	408357069	-	-	31.8 x 17.2 x 24.6 in.	665

1. Divided into two groups that can be controlled independently by the software.

2. Unit fits into standard 19-inch equipment racks. For tower configurations, the unit stands 17 inches high.

3. Also user-selectable for 100, 110 and 127 V.

Battery runtimes (in minutes)¹

1000 VA Model			
Load	Std Internal Batteries	(1) 24V EBM	(2) 24V EBMs
200 VA / 140 W	37	271	546
400 VA / 280 W	19	142	278
700 VA / 490 W	9	72	156
850 VA / 595 W	6	59	124
1000 VA / 700 W	5	48	104

1. This table provides typical information. Runtimes are approximate and may vary with equipment, configuration, battery age, temperature, etc.

Full Details on these units can be found in *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207. You can also go online to find out the latest details about UPS technology at <http://www.avayaups.com/avaya/default.asp>.

Terminal server installation

This section provides information on connecting adjunct equipment to a G700 or G350 Media Gateway with an S8300 Media Server using a terminal server ([Figure 34: Switch-to-adjunct LAN connectivity through a terminal server](#)). Avaya supports the IOLAN+ 104 terminal server.

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

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

Figure 34: Switch-to-adjunct LAN connectivity through a terminal server

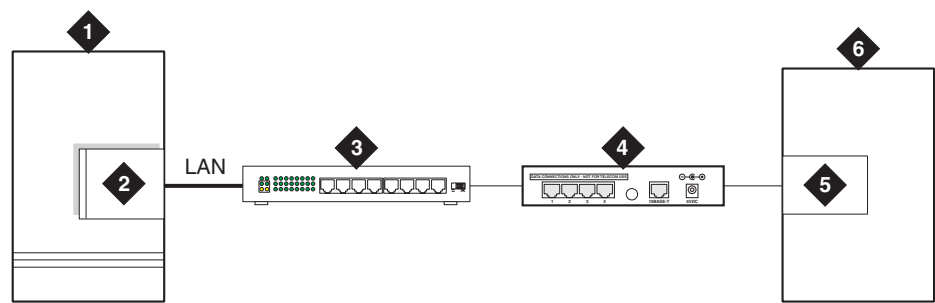


Figure notes:

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

Installing and administering the terminal server

Make sure you have all the equipment on site before the installation. You must have the hardware listed in [Table 25: Required equipment](#).

Table 25: Required equipment

Comcode	Description	Qty	Supplier
700015084	IOLAN+ 104 communications server	1	Avaya
NA	RJ45-to-DB25 connector for IOLAN+ (supplied with 700015084)	4	Avaya

1 of 2

Table 25: Required equipment (continued)

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

2 of 2

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

What are the distance limits for the terminal server

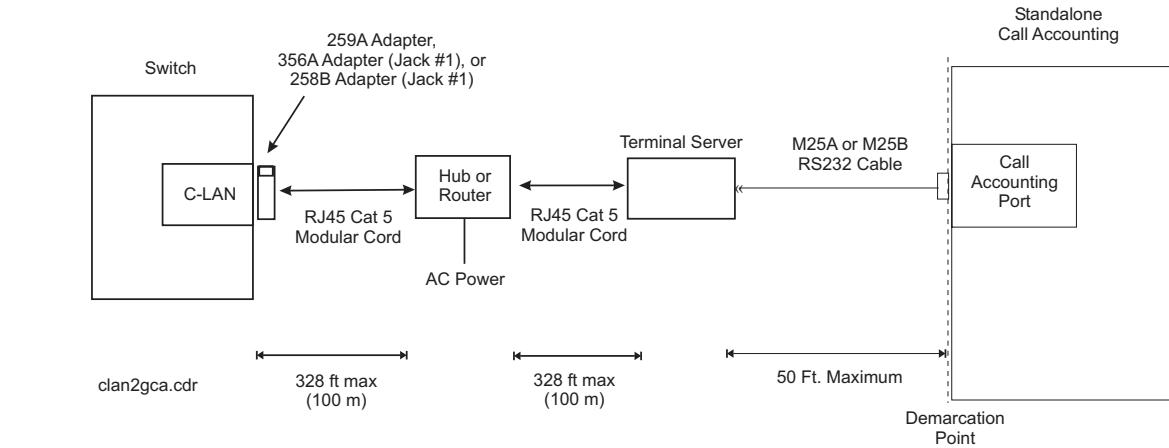
The distance limit from the switch to the LAN hub is 328 feet (100 meters). The distance limit from the LAN hub to the terminal server is 328 feet (100 meters). If installed, the limit from the terminal server to the adjunct is 50 feet (15 meters).

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

How is the terminal server cabling connected

[Figure 35](#) shows the connection between the terminal server port and a call accounting system.

Figure 35: Stand-alone call accounting system link using a terminal server



Note:

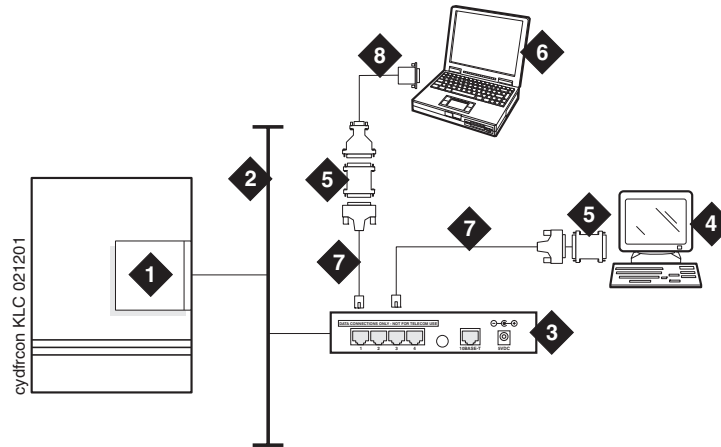
You can connect the S8300 Media Server directly to the terminal server with a data crossover cable. This connection eliminates the need for a hub or router in the middle, but the connection also allows the S8300 Media Server and the terminal server to communicate only with each other. With this connection,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

The general connection process requires:

- [Connecting the IOLAN+ to the adjunct and the LAN](#) on page 358
- [Administering the IOLAN+](#) on page 359
- Test the connectivity back through the switch

Connecting the IOLAN+ to the adjunct and the LAN

Connect the adjunct to the IOLAN+, using the RJ45-to-DB25 cable and the null modem. You can use a male/female adapter. See [Figure 36: Connecting an adjunct to the IOLAN+](#) on page 359.

Figure 36: Connecting an adjunct to the IOLAN+**Figure notes:**

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

Follow these typical steps:

Note:

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

To Connect the IOLAN+ to the adjunct and the LAN

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

Note:

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

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

Administering the IOLAN+

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

Note:

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

To connect the IOLAN+

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

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

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

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

To set up HyperTerminal on the computer

1. Open HyperTerminal.
2. Click on **File > Properties > Connect** tab.
In the Connect using: field, select **COM *n***
where ***n*** is the communication port your computer is using.
3. Click on **CONFIGURE**
Set the **bits per second** field to **9600**.
Set the **Flow control** field to **Hardware**.
4. Click **OK**.
5. Press **ENTER** to get the login prompt.

To administer the IOLAN+ the first time

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

```

Name: port 2                                CONNECTIONS MENU                                Terminal: 2

                                     Connection      Host

                                     1                *** FREE **
                                     2                *** FREE **
                                     3                *** FREE **
                                     4                *** FREE **

                                     *** Commands ***
                                     | Telnet      ^T|
                                     | Rlogin     ^R|
                                     | Port       ^P|
                                     | Admin mode ^A|
                                     | CLI        |
                                     | Lock       |
                                     | Logout    ^D|
                                     |=====|

IOLAN PLUS v4.02.00 a CDi                                iolan

```

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

```

Name: port 2                                ADMINISTRATION MENU                                Terminal: 2

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

Password     [          ]

IOLAN PLUS v4.02.00 a CDi                                iolan-st

```

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

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

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

** Administrator **		SERVER CONFIGURATION	Terminal: 2
Name	[iolan]	Debug mode	[0]
IP address	[123.45.67.89]		
Subnet mask	[222.222.0.0]		
Ethernet address	[00:80:d4:03:11:cd]	Ethernet interface	[AUTO]
Language	[English]		
Identification	[]		
Lock	[Disabled]		
Password limit	[5]		
CR to initiate	[No]		
SNAP encoding	[Disabled]		
Boot host	[]	Boot diagnostics	[Enabled]
Boot file	[]		
Init file	[]		
MOTD file	[]		
Domain name	[]		
Name server	[]	NS Port	[53]
WINS server	[]		

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

IOLAN PLUS v4.02.00 a CDi iolan

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

Leave the default settings for the other fields.

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

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

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

To reboot the IOLAN+

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

```

** Administrator **                ADMINISTRATION MENU                Terminal: 2

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

Port                [2  ]

IOLAN PLUS v4.02.00 a CDi                iolan

```

Note:

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

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

Navigating the IOLAN+ terminal server

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

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

Administering the gateway

Note:

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

To administer the gateway for IOLAN+

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

Note:

The following steps re-initialize the IOLAN+ so it knows it's connected to the LAN through your gateway.

5. Select **reboot** and press **ENTER**.
6. Press the space bar to restart the IOLAN+.

Administering an IOLAN+ port

Use this procedure when connecting an adjunct or serial COM port on a PC directly (locally) to the IOLAN+ (see [Figure 36: Connecting an adjunct to the IOLAN+](#) on page 359).

To administer an IOLAN+ port

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

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

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

** Administrator **		PORT SETUP MENU		Terminal: 2	
Hardware		Flow ctrl		Keys	
Speed	[9600]	Flow ctrl	[xon/xoff]	Hot	[^]] Intr [^C]
Parity	[None]	Input Flow	[Enabled]	Quit	[^@] Kill [^U]
Bit	[8]	Output Flow	[Enabled]	Del	[^@] Sess [^@]
Stop	[1]			Echo	[^@]
Break	[Disabled]	IP Addresses			
Monitor DSR	[Yes]	Src	[]	Mask	[]
Monitor DCD	[No]	Dst	[]		
User		Options		Access	
Name	[port 2]	Keepalive	[No]	Access	[Remote]
Terminal type	[undef]	Rlogin/Telnet	[Telnet]	Authentication	[None]
TERM	[]	Debug options	[No]	Mode	[Raw]
Video pages	[0]	Map CR to CR LF	[No]	Connection	[None]
CLI/Menu	[CLI]	Hex data	[No]	Host	[]
Reset Term	[No]	Secure	[No]	Remote Port	[0]
		MOTD	[No]	Local Port	[5101]
IOLAN PLUS v4.02.00 a CDi				iolan	

5. Fill in the following fields.

Leave the default settings for the other fields.

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

Telephones and adjunct systems

- **Host:** *leave blank or enter S8300 Media Server IP Address*
 - **Remote Port:** *0*
 - **Local Port:** *must match the value of Remote Port on the IP Services screen of the Communication Manager software*
6. Press **ENTER** and select **Save & Exit** to effect the changes.
 7. Press **ENTER** again to view the **Administration Menu**.
 8. Select **kill** to disable the port connection.
 9. Repeat the steps for each additional port you want to administer.
 10. When administration is complete, from the **Connections Menu**, select **logout** (or press **Ctrl D**).
 11. Close HyperTerminal.

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

Testing connectivity through the IOLAN+

To test connectivity through the IOLAN+

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

Note:

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

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

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

If not, check all your connections and administration fields.

```

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

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

```

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

Potential failure scenarios and repair actions

If a link goes down between the terminal server and the switch, you must reboot the terminal server for the link come back up. If you are performing a software upgrade or if a system reset occurs, you must reboot the terminal server to restore the link. See [To reboot the IOLAN+](#) on page 363 for instructions.

change node-names ip

Page 1 of 1

NODE NAMES			
Name	IP Address	Name	IP Address
1. switch-clan_____	123.456.7 .89	17. _____	____.____.____.____
2. callacctg_____	123.456.9 .00	18. _____	____.____.____.____
3. termserver_____	123.456.11 .00	19. _____	____.____.____.____
4. pmslogpc_____	123.456.78 .00	20. _____	____.____.____.____
5. _____	____.____.____.____	21. _____	____.____.____.____
6. _____	____.____.____.____	22. _____	____.____.____.____
7. _____	____.____.____.____	23. _____	____.____.____.____
8. _____	____.____.____.____	24. _____	____.____.____.____
9. _____	____.____.____.____	25. _____	____.____.____.____
10. _____	____.____.____.____	26. _____	____.____.____.____
11. _____	____.____.____.____	27. _____	____.____.____.____
12. _____	____.____.____.____	28. _____	____.____.____.____
13. _____	____.____.____.____	29. _____	____.____.____.____
14. _____	____.____.____.____	30. _____	____.____.____.____
15. _____	____.____.____.____	31. _____	____.____.____.____
16. _____	____.____.____.____	32. _____	____.____.____.____

Administering IP services

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

To administer IP services

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

change ip-services						Page	1 of	3
IP SERVICES								
Service	Enabled	Local	Local	Remote		Remote		
Type		Node	Port	Node		Port		
CDR1		procr	0	callacctg		5101		

3. In the **Local Node** field, enter the node name for the switch.
In this example, enter **procr**.
4. The **Local Port** field defaults to 0 for all client applications.
You cannot make an entry in this field.
5. In the **Remote Node** field, enter the node name for the adjunct, as administered on the **Node Names** screen.
For the call accounting application, type **callacctg**.
6. In the **Remote Port** field, enter the TCP listen port assigned to the adjunct.
The recommended value for CDR1 is 5101.

Note:

This number must match the port administered on the end device. If you are using the Downloadable Reliable Session-Layer Protocol tool, this must match the port administered in the Server application. If you are using a terminal server, this number must match the **Local Port** number on the Port Setup menu. Consult the documentation for your Call Accounting system to determine the appropriate port for the CDR device.

7. Go to Page 3 and type **n** in the **Reliable Protocol** field for the CDR Service Type.
You do not use RSP with a terminal server.

change ip-services						Page	3 of	3
SESSION LAYER TIMERS								
Service	Reliable	Packet	Resp	Session	Connect	SPDU	Connectivity	
Type	Protocol	Timer		Message	Cntr	Cntr	Timer	
CDR1	n	3		1		1	1	

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

Call detail recording (CDR)

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

Connecting CDR equipment

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

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

Note:

A printer or customer premises equipment (CPE) can also be used as the output receiving device. Please see [Printers](#) on page 375 of this book for instructions on using a printer.

Administering CDR data collection

Note:

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

To administer CDR Data Collection

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

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

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

2. Access the **IP Services** screen in Communication Manager (see [Administering IP services](#) on page 368), and do the following:

- a. In the **Service Type** field, enter **CDR1** or **CDR2**.
- b. In the **Local Node** field, enter **procr**.
- c. The **Local Port** field defaults to 0 for all client applications.

You cannot make an entry in this field.

- d. In the **Remote Node** field, enter the node name you assigned to the CDR adjunct in step 2.
 - e. In the **Remote Port** field, enter the port number used by the CDR adjunct determined in step 1.
3. Go to Page 3 and do the following:
- a. Enter **y** in the **Reliable Protocol** field if you have a CDR application using RSP.
Enter **n** if the CDR adjunct is connected through a terminal server.
 - b. If RSP is being used, complete the **Packet Resp Timer** and **Connectivity Timer** fields with a reasonable value that matches the network condition (recommended values are **30** and **60** seconds, respectively).
 - c. Accept the defaults in the other fields.
4. Administer CDR parameters as described in [Administering CDR parameters](#) on page 371.

Administering CDR parameters

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

To administer CDR parameters

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

The **CDR System Parameters** screen appears.

change system-parameters cdr	Page 1 of 1
CDR SYSTEM PARAMETERS	
Node Number (Local PBX ID):	CDR Date Format: month/day
Primary Output Format: unformatted	Primary Output Endpoint: CDR1
Secondary Output Format: unformatted	Secondary Output Endpoint: CDR2
Use ISDN Layouts? n	EIA Device Bit Rate: 9600
Use Enhanced Formats? n	Condition Code 'T' for Redirected Calls? n
Modified Circuit ID Display? n	Remove # From Called Number? n
Record Outgoing Calls Only? y	Intra-switch CDR? n
Suppress CDR for Ineffective Call Attempts? y	CDR Call Splitting? y
Disconnect Information in Place of FRL? n	Outg Attd Call Record? y
	Interworking Feat-flag? n
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n	
	Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n	
Record Called Agent Login ID Instead of Group or Member? n	
Inc Trk Call Splitting? n	
Record Non-Call-Assoc TSC? n	Call Record Handling Option: warning
Record Call-Assoc TSC? n	Digits to Record for Outgoing Calls: dialed
Privacy - Digits to Hide: 0	CDR Account Code Length: 4

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

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

3. In the **Primary Output Endpoint** field, type **CDR1**.
4. If you use a secondary output device, and that device is also connected through TCP/IP, complete the **Secondary Output Format** field.

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

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

Testing the switch-to-adjunct link

You can use the test, status, busyout and release commands to find and correct problems with CDR links. For more information about these commands, see *Maintenance Commands for Avaya Communication Manager 3.0, Media Gateways and Servers*, 03-300431.

```
status cdr-link
                    CDR LINK STATUS
                Primary                Secondary
Link State: up                extension not administered
Maintenance Busy? no
```

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

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

Additional administration procedures for CDR equipment are provided in the *Administrator Guide for Avaya Communication Manager*, 03-300509.

Reliable Data Transport Tool (RDTT) package

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

What does the RDTT package contain

The RDTT package consists of the following:

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

This application is designed to help you test the reliable session protocol without use of an Avaya Media Server.

- The Server application (Server.exe)

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

- User Guide

This document contains information about the client and server applications.

Downloading the RDTT package

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

To download the RDTT package

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

It is approximately 1.6 to 2.0MB in size.

Installing the RDTT package

To install the RDTT package

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

The Install Shield Wizard steps you through the installation.

2. When prompted to select Client or Server, select both programs.
3. Continue with the installation.

Use the default destination folder and program folder.

Administering the RDTT package

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

Related topics

See the following topics related to CDR:

- Chapter 16, “Collecting Billing Information,” in *Administrator Guide for Avaya Communication Manager*, 03-300509.
- “Call Detail Recording” in Chapter 21, “Features and Technical Reference” in *Administrator Guide for Avaya Communication Manager*, 03-300509.

Printers

For connecting a printer to a G700 or G350 Media Gateway, see [Terminal server installation](#) on page 356 for more information.

DS1/T1 CPE loopback jack

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

Note:

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

Note:

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

This section covers:

- [Installing a loopback jack](#) on page 376
- [Administering a loopback jack](#) on page 378
- [Testing a loopback jack with a smart jack](#) on page 378
- [Testing a loopback jack without a smart jack](#) on page 387
- [Configurations using fiber multiplexers](#) on page 390

Installing a loopback jack

You can use one of two installation options:

- [Installing a loopback jack with a smart jack](#) on page 376
- [Installing a loopback jack without a smart jack](#) on page 377

Installing a loopback jack with a smart jack

Use one of the following installation methods:

- Install the loopback jack at the interface to the smart jack, if possible.
This position provides maximum coverage of CPE wiring when remote loopback tests are run.
- If the smart jack is not accessible, install the loopback jack at the extended demarcation point.

- If there is no extended demarcation point, install the loopback jack directly at the network interface point as shown in [Figure 37](#).
- If there is an extended demarcation point and the smart jack is not accessible, install the loopback jack as shown in [Figure 38](#).
- If there is an extended demarcation point, but the smart jack is accessible, install the loopback jack as shown in [Figure 39](#).

To install the loopback jack with a smart jack

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

See [Figure 37](#) through [Figure 39](#).

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

Note:

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

Installing a loopback jack without a smart jack

Use one of the following installation methods:

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

Refer to [Figure 40](#) and [Figure 41](#).

To install the loopback jack without a smart jack

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

See [Figure 40](#) through [Figure 41](#).

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

Note:

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

Administering a loopback jack

To administer a loopback jack

1. At the management terminal, type `change ds1 location`
where `location` is the DS1 interface circuit pack corresponding to the loopback jack.
2. Verify that the **near-end CSU** type is set to `integrated`.
3. On page 2 of the form, change the **supply CPE loopback jack power** field to `y`.
Setting this field to `y` informs the technician that a loopback jack is present on the facility and allows the technician to determine that the facility is available for remote testing.
4. Enter `save translation` to save the new information.

Testing a loopback jack with a smart jack

The loopback jack and smart jack isolate faults by dividing the DS1 span into three sections (see [Figure 37](#) through [Figure 39](#)).

These three sections are:

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

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

Testing the DS1 span from the ICSU to the loopback jack

The DS1 span test has 2 parts:

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

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

Checking the integrity of local equipment

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

To test the DS1 span

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

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

2. Type **busyout board XXXVS**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Testing the integrity of data sent over the loop

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

Note:

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

To test the integrity of data sent over the loop

1. At the SAT, type `clear meas ds1 loop XXXVS` to zero out the bit-error counter.
where **XXX** is the administered number of the G700 or G350 (for example, **002**), and **VS** is the slot number on the G700 or G350 of the Media Module (for example, **V3**).
2. Type `clear meas ds1 log XXXVS` to zero out the performance measurement counter.
3. Type `clear meas ds1 esf XXXVS` to zero out the ESF error count.
4. Type `list meas ds1 sum XXXVS` to display the bit error count.
5. Step through [Table 26: DS1 Troubleshooting](#) to troubleshoot.

Table 26: DS1 Troubleshooting

Condition	Solution
The value of the Test: cpe-loopback-jack field is <code>Pattern 3-in-24</code>	The loopback jack test is active.
The value of the Synchronized field is <code>N</code>	Retry the test 5 times.
The value of the Synchronized field remains <code>N</code> after 5 tries.	Excessive bit errors are likely. Check for intermittent connections or broken wires in an SPE receive or transmit pair, and repair as necessary. Then repeat Step 1.
The value of the Bit-error count field is <i>non-zero</i>	Repeat Step 1 several times.
The value of the Synchronized field is <code>Y</code>	The DS1 circuit pack has synchronized to the looped 3-in-24 pattern and is counting bit errors in the pattern.
1 of 2	

Table 26: DS1 Troubleshooting (continued)

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

2 of 2

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

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

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

7. Type `list meas ds1 sum XXXVS` to display the bit error count again.

8. Step through [Table 27: DS1 Bit-error count troubleshooting](#) on page 381 to troubleshoot.

Table 27: DS1 Bit-error count troubleshooting

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

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

Wait about 30 seconds for the DS1 to reframe on the incoming signal and clear DS1 facility alarms. Use [Table 28: Evaluation of DS1 loopback test results](#) on page 382 to evaluate the test results and to determine the solution.

Table 28: Evaluation of DS1 loopback test results

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

To restore DS1 administration

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

To release the DS1 circuit pack

1. At the SAT, type `release board xxxvs`.
2. Leave the loopback jack in place.

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

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

1. Have the service provider run a smart-jack loopback test against the network interface wiring that links the smart jack to the CO (section 3 in [Figure 37](#) through [Figure 39](#)).
2. If the tests fails, there is a problem on the network side.

Have the service provider correct it.

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

Note:

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

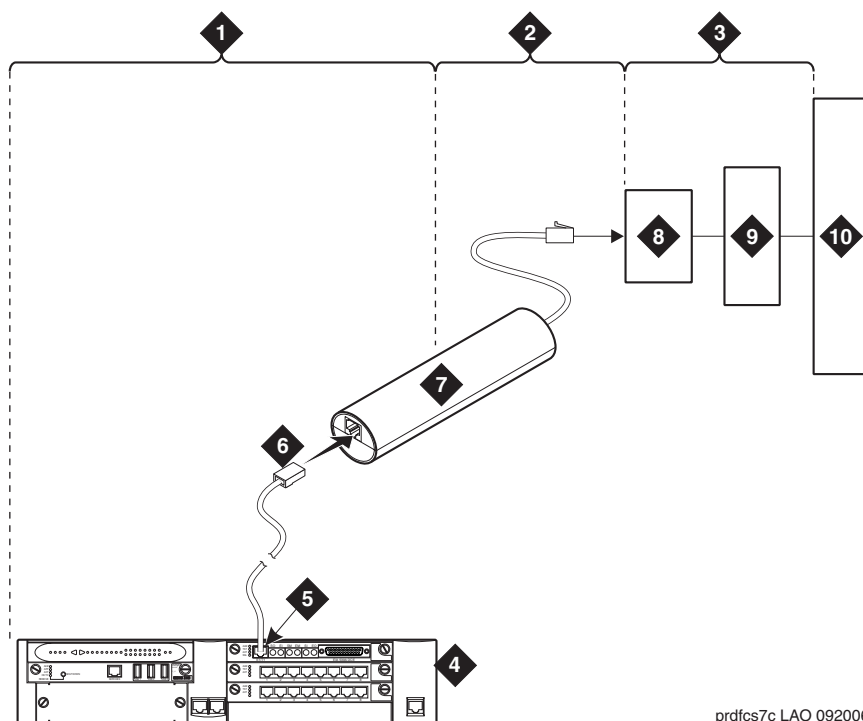
Test the short length of customer premises wiring between the loopback jack and the smart jack (Section 2 in the following 3 figures) using a loopback that overlaps this section of the span.

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

1. Have the DS1 service provider at the CO end run a local ICSU line loopback test.
2. Have the DS1 service provider at the CO end run a local DS1 payload loopback test.
3. Run a far-end MM710 line loopback, using the following procedure:
 - a. From the SAT, type `test ds1-loop XXXVS far-csu-loopback-test-begin`, where **xxx** is the administered number of the G700 (for example, **002**), and **vs** is the slot number on the G700 of the Media Module (for example, **V3**).
 - b. Examine the bit-error counts, as in [Testing the integrity of data sent over the loop](#) on page 380.
 - c. Type `test ds1-loop location end-loopback/span-test` to terminate the test.

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

Figure 37: Network interface at smart jack for an MM710 multi-media module

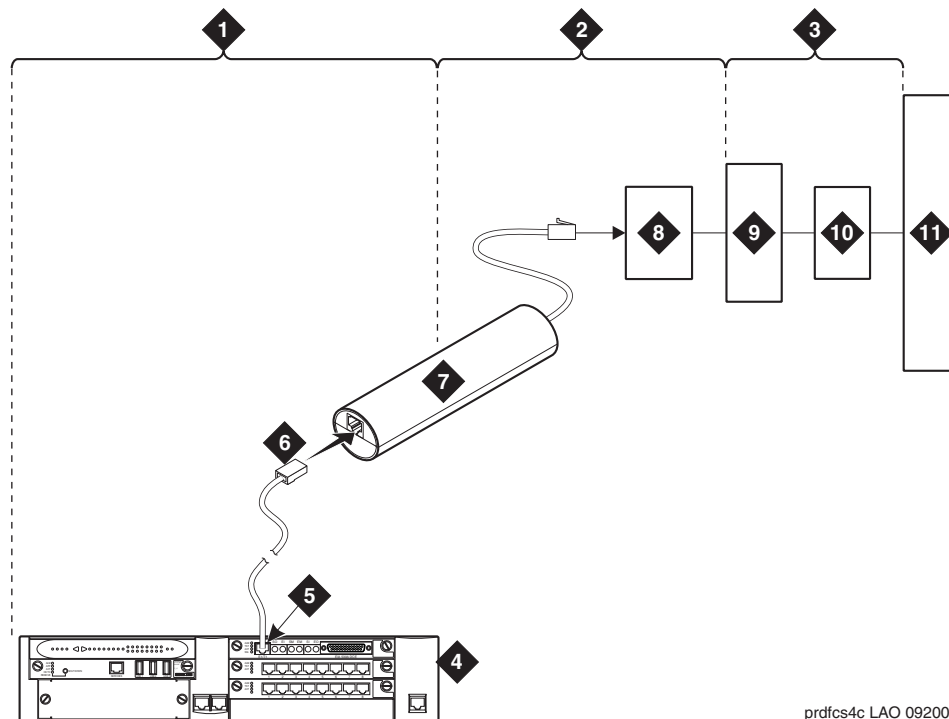


prdfcs7c LAO 092006

Figure notes:

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

Figure 38: Network interface at extended demarcation point (smart jack inaccessible) for an MM710 multi-media module

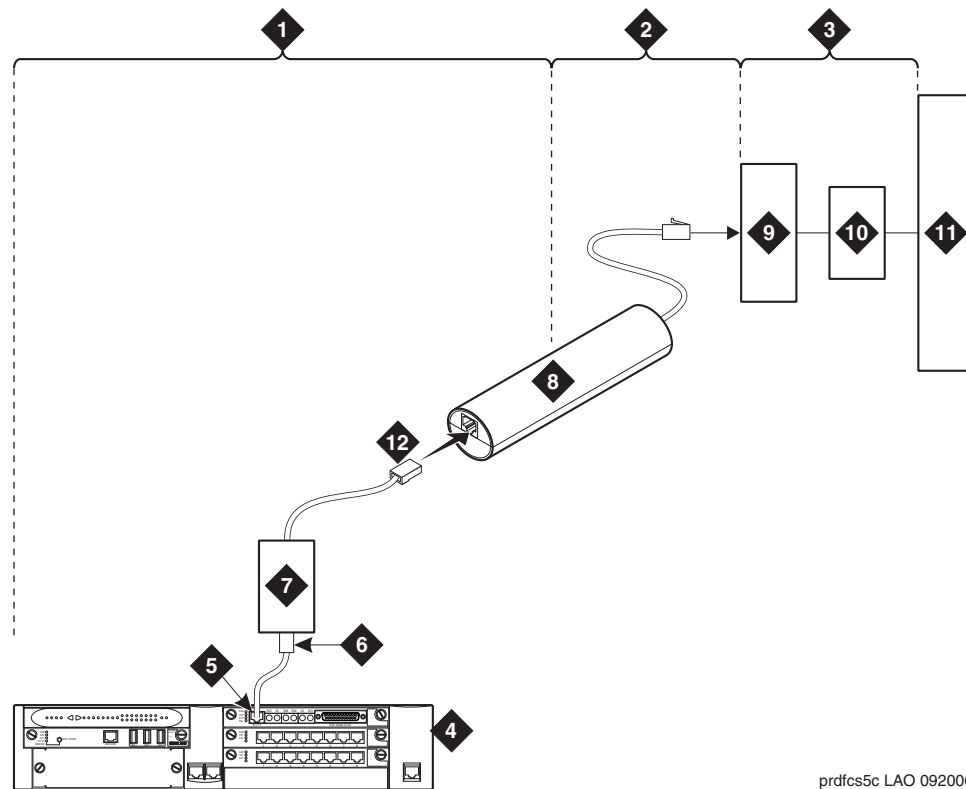


prdfcs4c LAO 092006

Figure notes:

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

Figure 39: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module



prdfcs5c LAO 092006

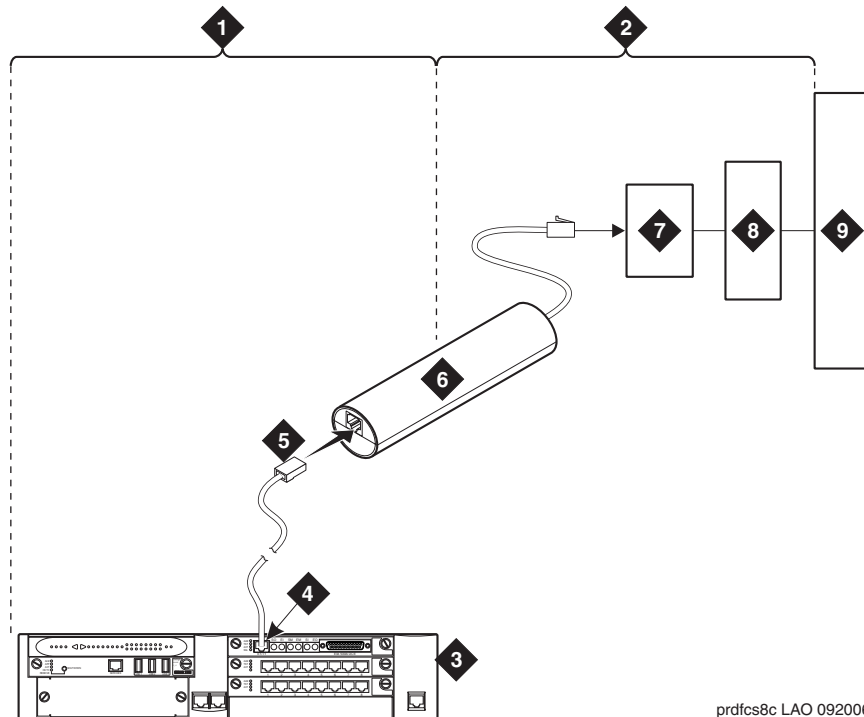
Figure notes:

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

Testing a loopback jack without a smart jack

When the loopback jack is added to a span that does not contain a smart jack, the span is divided into 2 sections: from the MM710 to the loopback jack and from the loopback jack to the central office (CO). Section 2 includes the short cable from the loopback jack to the dumb block demarcation point (part of the loopback jack). This cable is the only part of Section 2 that is part of customer premises wiring. It is not covered in the loopback jack's loopback path. See [Figure 40](#) and [Figure 41](#).

Figure 40: Network interface at “dumb” block for an MM710 multi-media module

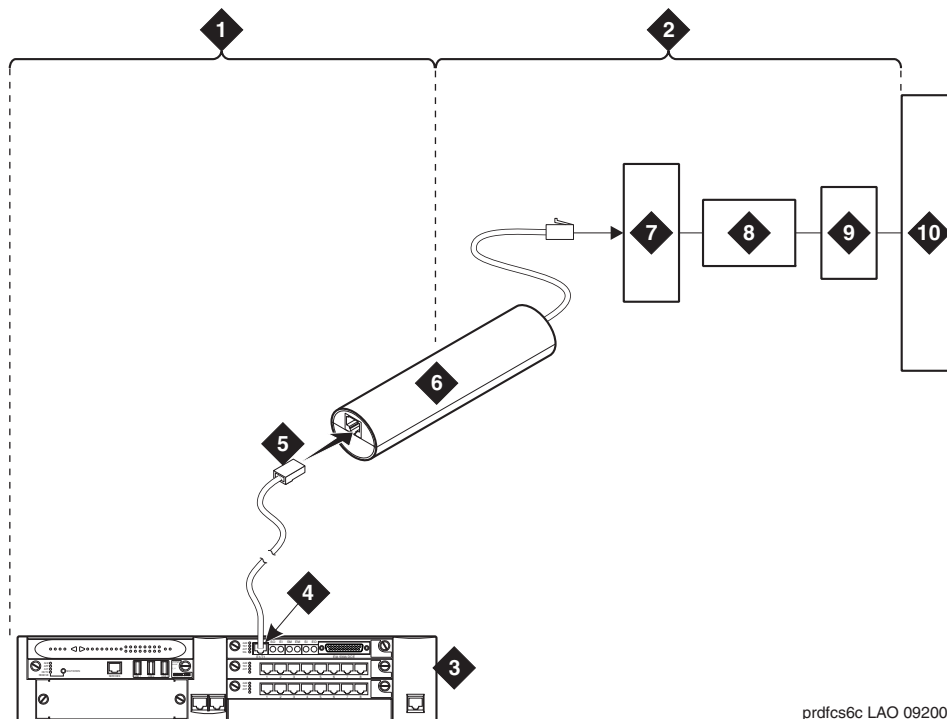


pdfcs8c LAO 092006

Figure notes:

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

Figure 41: Network interface at “dumb” block with repeater line to fiber MUX for an MM710 multi-media module



pdfcs6c LAO 092006

Figure notes:

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

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

To test a loopback jack without a smart jack

1. Test customer premises wiring from the MM710 to the loopback jack, as described in [Testing the DS1 span from the loopback jack to the smart jack](#) on page 383.
2. Test the loopback jack-to-*dumb* block and *dumb* block-to-CO wiring (section 2 in [Figure 40](#) and [Figure 41](#)).

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

- The local ICSU's line loopback, which the DS1 service provider at the CO end typically activates, tests, and then deactivates.
- The local DS1 interface's payload loopback, which the DS1 service provider at the CO end activates and tests.
- The far-end MM710's line loopback:
 - a. At the SAT type test `ds1-loop location far-csu-loopback-test-begin` to activate this test,
 where *location* is the DS1 interface circuit pack corresponding to the loopback jack.
 - b. Type test `ds1-loop location end-loopback/span-test` to terminate this test,
 where *location* is the DS1 interface circuit pack corresponding to the loopback jack.

Bit error counts are examined as described in [Testing the DS1 span from the ICSU to the loopback jack](#) on page 378. This test only isolates problems to Section 2 wiring if there are no problems in the wiring between the far-end CO and the far-end ICSU. Coordinate this test with the DS1 service provider.

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

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

- a. Identify and contact the DS1 service provider.
- b. Inform the DS1 provider that loopback tests of the CPE wiring to the “dumb” block (section 1) showed no problems.
- c. If the far-end MM710 line loopback test failed, inform the DS1 provider.
- d. Request that the DS1 provider perform a loopback test of their portion of the Section 2 wiring by sending someone out to loop Section 2 back to the CO at the “dumb” block.

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

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

Configurations using fiber multiplexers

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

Fiber MUXs can take the place of Interface termination feeds as shown in [Figure 37](#) through [Figure 40](#). Test these spans using the same procedures as metallic spans.

Note:

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



Important:

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

Checking for the presence of DC

To check for the presence of DC:

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

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

External modems

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

Recommended modems include:

- [Multi-Tech MT5634ZBA-USB-V92](#)

This section covers:

- [Hardware required when configuring modems](#) on page 391
- [Multi-Tech MT5634ZBA-USB-V92](#) on page 391
- [Multi-Tech MT5634ZBA-V92-GLOBAL](#) on page 392
- [Administering Multi-Tech modems](#) on page 392

Hardware required when configuring modems

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

Note:

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

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

Proceed as follows:

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

Multi-Tech MT5634ZBA-USB-V92

Avaya recommends using a Multi-Tech USB modem, model MT5634ZBA-USB-V92, with an S8300/700, S8500, or S8700/S8710 configuration. This modem is used for sending alarms, as well as for remote dial up to the server for maintenance and administration.

Configuring the MT5634ZBA-USB-V92 modem

In the United States, the Multi-Tech MT5634ZBA-US-V92 modem gets configured automatically through the USB port with the factory defaults. No special configuration is necessary. In a non-US country, the modem may require settings specific to the country in which the modem will be used.

Multi-Tech MT5634ZBA-V92-GLOBAL

Avaya recommends using a Multi-Tech serial modem, model MT5634ZBA-V92-GLOBAL, with a G350 media gateway.

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

Administering Multi-Tech modems

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

For the full range of modem options, see the *Administrator Guide for Avaya Communication Manager*, 03-300509.

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

The customer-provided busy tone disconnect adjunct detects busy tone disconnects of incoming calls on loop-start, 2-wire, analog trunks. In some non-U.S. countries where a G700 or G350 Media Gateway is used, the PSTN sends busy tone as the disconnect signal. Therefore, the S8300 Media Server, G700 Media Gateway, or G350 Media Gateway requires a busy tone disconnect adjunct. [Figure 42](#) shows typical connections.

Figure 42: Typical cabling for busy tone disconnect

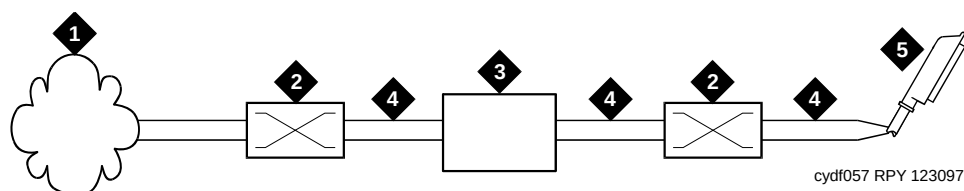


Figure notes:

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

Music-on-hold

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

- [Installing an unregistered music source on a G700 or G350 Media Gateway](#) on page 394
- [Installing a registered music source on a G700 or G350 Media Gateway](#) on page 397

Music-on-hold can be provided:

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

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

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

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

[Figure 43](#) and [Figure 44](#) show the connections for the music-on-hold feature on a G700 Media Gateway for an unregistered source.

Note:

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

Note:

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

Figure 43: Unregistered music-on-hold equipment connecting to KS-23395-L3 for a G700 Media Gateway

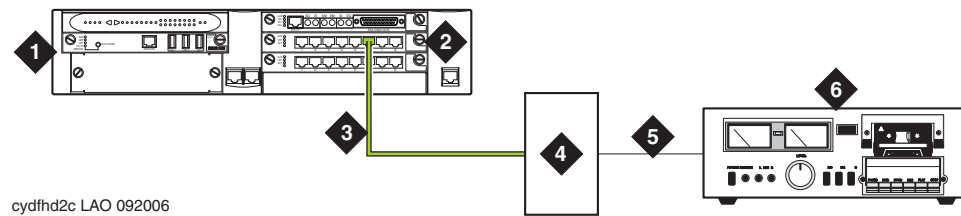


Figure notes:

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

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

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.
For a G350 Media Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the other end of the RJ-45 cable to a KS-23395-L3 coupler.
3. Connect the KS-23395-L3 coupler to the customer-supplied music source.
Follow the manufacturer's instructions to properly connect the music source to the KS-23395-L3 coupler. Normally, you simply use an RCA cord.
4. Administer the switch for the new equipment.

Figure 44: Unregistered music-on-hold equipment connecting to KS-23395-L4 for a G700 Media Gateway

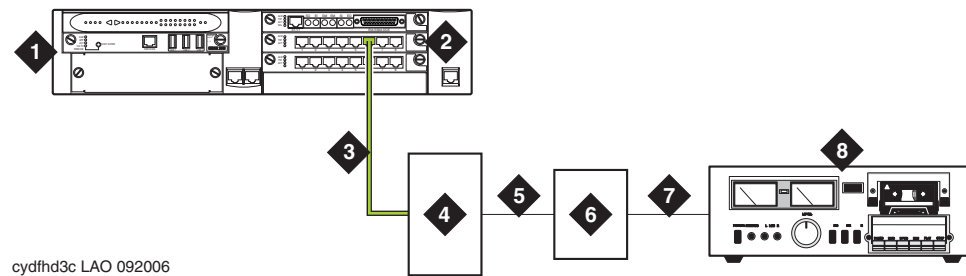


Figure notes:

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

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

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.
For a G350 Media Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the other end of the RJ-45 cable to a KS-23395-L4 coupler.
3. Connect the KS-23395-L4 coupler to the 909A/B universal coupler using a 8-pair modular cord.
4. Connect the 909A/B universal coupler to the music source using a 8-pair modular cord.
5. Administer the switch for the new equipment.

Note:

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

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

[Figure 45](#) show the connections for the music-on-hold feature on a G700 Media Gateway for a registered source.

Note:

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

Note:

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

Figure 45: Registered music-on-hold equipment connecting to KS-23395-L4 for a G700 Media Gateway

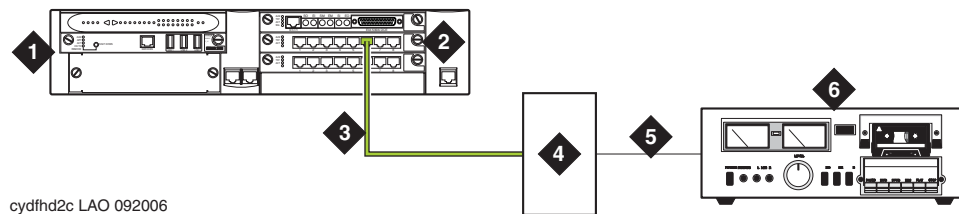


Figure notes:

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

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

1. Connect one end of an RJ-45 cable to a port in the MM711 Analog Media Module.
For a G350 Media Gateway only, connect the RJ-45 cable to a port in an MM714 Analog Media Module or a fixed analog (LINE 1 or 2) port on the G350 front panel.
2. Connect the KS-23395-L4 coupler to the customer-supplied music source.
Normally, you simply use a 8-pair modular cord.
3. Administer the switch for the new equipment.

Paging and announcement equipment

This section provides information on loudspeaker paging.

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

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

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

[Figure 46](#) shows the connections for loudspeaker paging, dial dictation, or recorded announcement features on a G700 or G350 Media Gateway.

Figure 46: Typical loudspeaker equipment connections for a G700 or G350 Media Gateway

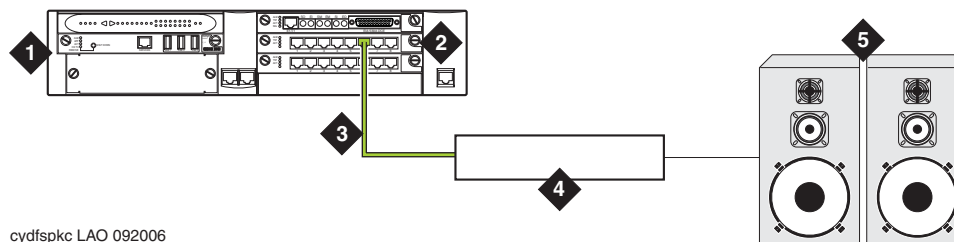


Figure notes:

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

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

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

Note:

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

Adjunct Information Sources

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

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

Call Management System

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

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

INTUITY AUDIX Messaging Systems

For information on installing INTUITY AUDIX Messaging systems, see one of the following:

- For INTUITY AUDIX Release 5.1 Messaging, see *INTUITY Messaging Solutions Release 5 Installation for New Systems* on the *INTUITY Messaging Solutions Release 5 Documentation CD-ROM*, 585-313-803.
- For INTUITY AUDIX LX Messaging, see *INTUITY AUDIX LX Installation Checklist* on the *INTUITY AUDIX LX Release 1 Documentation CD-ROM*, 585-313-818.
- *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532.
- For IA770 INTUITY AUDIX Messaging R1.3 (when available), go to <http://support.avaya.com>.

Avaya Modular Messaging System

For information on installing Avaya Modular Messaging systems, see *Modular Messaging Release 2.0 Documentation CD-ROM*, 11-300121.

ASAI and DEFINITY LAN Gateway

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

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

Avaya Interactive Response

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

Avaya EC500 Extension to Cellular and Off-PBX Stations

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

SIP Enablement Services

For information on installing Avaya SIP Enablement Services (SES), see the *SIP Enablement Services Implementation Guide*, 16-300140, and *SIP Support in Avaya Communication Manager 4.0*, 555-245-206.

Seamless Converged Communications across Networks (SCCAN)

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

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

Call Accounting Systems

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

Section 3: G700 installation and upgrades - manual procedures

This section contains manual procedures to install or upgrade an Avaya G700 Media Gateway controlled by an Avaya S8300, S8500, or S8700-series Media Server. Information on connecting telephones and adjuncts to the G700 is presented in [Chapter 7: Telephones and adjunct systems](#).

This section is organized into the following chapters:

- [Chapter 8: Manual installation of a new G700 with an S8300](#)
- [Chapter 9: Manual installation of a new G700 without an S8300](#)
- [Chapter 10: Manual upgrade of an S8300A and G700 to R4.0](#)
- [Chapter 11: Manual upgrade of an existing S8300B or S8300C and G700 to R4.0](#)
- [Chapter 12: Manual upgrade of an existing S8300B and G700 to S8300C with R4.0](#)
- [Chapter 13: Manual upgrade of an existing G700 without an S8300 to R4.0](#)

Note:

Automated procedures to perform many of these tasks, using Avaya wizard tools may be found in [Section 2: G700 installation and upgrades - wizards](#).

Chapter 8: Manual installation of a new G700 with an S8300

This chapter covers the manual procedures to install a new Avaya G700 Media Gateway with an Avaya S8300 Media Server. The S8300 can be configured as either the primary controller or as a local survivable processor (LSP).

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

The G700 ships with the firmware installed on the G700 processors and media modules. However, you may need to upgrade Communication Manager, G700 firmware, and/or media module firmware if the latest available versions are not currently installed.

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

Note:

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

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

- The version of Communication Manager on the LSP must be the same as, or later than, the version running on the primary controller.
- For an LSP, you administer Communication Manager translations on the primary controller, *not* on the LSP. The primary controller then copies the translations to the LSP.

Installation Overview

About software and firmware files

A new S8300 Media Server comes with a blank hard drive. The G700 components should have current releases of firmware installed. It may be necessary to install a service pack on the S8300 after installing the Communication Manager software, and/or to upgrade the G700 and media module firmware.

Communication Manager software is distributed on a CD-ROM that you take to the site. Additional files that may be needed are the most recent versions of the software service pack file and G700 firmware files. You may need to obtain these files from the Avaya Support web site.

About access to the Communication Manager software distribution CD

The R4.0 Communication Manager software and other files needed for the R4.0 installation are on the Communication Manager software distribution CD that you take to the customer site. Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate.

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

Tasks to install the S8300 and the G700

Before going to the customer site

- [Obtaining a USB DVD or CD-ROM drive](#) on page 409
- [Getting information that the project manager provides](#) on page 409
- [Getting the serial Number of the G700, if necessary](#) on page 409
- [Checking for and FTP/SCP/SFTP server or compact flash for backing up data](#) on page 409
- [Obtaining service pack files, if needed](#) on page 410

- [Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary](#) on page 411
- [Obtaining Ethernet interface IP address and subnet mask](#) on page 412
- [Completing the RFA process \(Obtaining license and password file\)](#) on page 412
- [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 413

Install the S8300

- [Inserting the S8300](#) on page 415
- [Setting telnet parameters](#) on page 416
- [Remastering the hard drive and installing the software](#) on page 417
- [Accessing the S8300](#) on page 420
- [Verifying Software Version](#) on page 420
- [Copying Files to the S8300 hard drive](#) on page 421
- [Downloading optional language files, if needed](#) on page 423
- [Verifying the Time, Date, and Time Zone](#) on page 423
- [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 424
- [Configuring the S8300](#) on page 428
- [Providing the keys.install File \(If Necessary\)](#) on page 440
- [Installing the license and authentication files](#) on page 441
- [If the server is an LSP, stop and start Communication Manager](#) on page 443
- [Installing security files and Communication Manager service packs, if any](#) on page 443
- [Saving Translations](#) on page 445

Configure the G700 Media Gateway

- [Assigning IP Addresses of the G700 Media Gateway Components](#) on page 446
- [Checking for IP connections](#) on page 451
- [Setting up the Controller List for the G700](#) on page 452
- [Setting the LSP Transition Points](#) on page 454
- [Configuring an X330 Expansion Module \(If Necessary\)](#) on page 455

Install new firmware on the G700

- [Verifying the Contents of the tftpboot Directory](#) on page 456
- [Determining which firmware to install on the G700](#) on page 456
- [Installing New Firmware on the P330 Stack Processor](#) on page 458
- [Installing new firmware on the G700 Media Gateway Processor](#) on page 459

- [Installing new firmware on the media modules](#) on page 461
- [Setting rapid spanning tree on the network](#) on page 463

Administer an S8300 primary controller

- [Assigning Node Names and IP Addresses for the LSPs](#) on page 465
- [Administering Network Regions](#) on page 466
- [Associating LSPs with Network Regions](#) on page 467
- [Administering IP Interfaces](#) on page 468
- [Identifying LSPs to the S8300 primary controller](#) on page 469

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

- [Assigning Node Names and IP Addresses for the C-LANs and LSPs](#) on page 471
- [Administering Network Regions](#) on page 472
- [Assigning LSPs to the Network Regions](#) on page 474
- [Administering IP Interfaces](#) on page 475
- [Identifying the Survivable Processor on the primary controller](#) on page 479

Administer the media gateway

- [Administering the Media Gateway](#) on page 480

Set up alarming

- [Configuring the primary server to report alarms to a services support agency](#) on page 486
- [Configuring the G700 Media Gateway to send its traps to a network management system \(NMS\)](#) on page 487

Complete the installation of the S8300 (if the primary controller

- [Updating IA770 INTUITY AUDIX Messaging, if installed](#) on page 489
- [Backing up the system](#) on page 492
- [If using IA770, administer Communication Manager for Integrated Messaging](#) on page 494
- [Complete the Installation Process \(for an S8300 LSP\)](#) on page 494

Before Going to the Customer Site

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

Obtaining a USB DVD or CD-ROM drive

Upgrading Communication Manager on an S8300 to release 3.0 requires remastering the S8300B/C hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB DVD or CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD or CD-ROM drive at the site.

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Getting the serial Number of the G700, if necessary

For a new installation of a G700 with an S8300, you need the serial number of the G700 Media Gateway in order to complete the creation of the customer's license file on the rfa.avaya.com web site. To get this number, look for the serial number sticker on the back of the G700 chassis. If the unit is delivered directly to the customer and you will not have phone or LAN line access from the customer site to access the rfa.avaya.com web site, this task will require a preliminary trip to the customer site.

Checking for and FTP/SCP/SFTP server or compact flash for backing up data

During the installation and upgrade procedures, you must back up the system data to an FTP, SFTP, or SCP server, or to the USB Compact Flash drive. You use a server on the customer's LAN for backups.

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



Important:

Before going to the customer site, make sure that you can use either a customer server for backups or a compact flash card.

Obtaining service pack files, if needed

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

Service packs may or may not be needed, depending on the release of Communication Manager. For both new installations and upgrades, you may need to install a service pack after the installation or upgrade. For an upgrade, you may need a service pack before the upgrade as well.

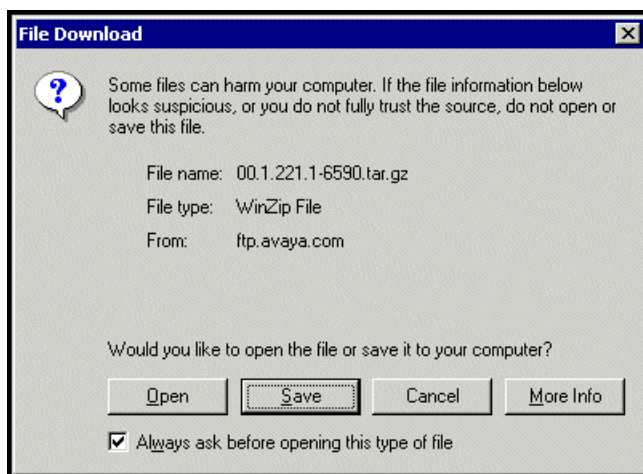
To download a pre-upgrade service pack

1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access <http://www.avaya.com/support> on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At the Avaya support site, select the following links:
 - a. **Find documentation and downloads by product name**
 - b. **S8300 Media Server**
 - c. **Downloads**
 - d. **Software downloads**
4. In the **Software Downloads** list, click on the link for the appropriate Communication Manager release (for example, **Avaya Communication Manager Software Updates for 4.0**).
5. Scroll down the page to find a link called **Latest Avaya Communication Manager x.x.x Software Update** (where x.x.x is the release number).

After this link, there should be a link starting with "PCN: "Click on this link to read about the release and software load to which this service pack applies.
6. Click on **Latest Avaya Communication Manager x.x.x Software Update** (where x.x.x is the release that is currently running on the S8300).

The File Download window displays.

File download window



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

Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary

If IA700 will be installed, determine whether a service pack is needed and/or optional languages are used. If so, obtain the data files.

Obtaining an IA770 service pack file

If an IA770 service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an IA770 service pack file

To obtain an IA770 service pack file

1. On the Avaya Support Web site, click on **Find Documentation and Downloads by Product Name**.
2. Under the letter "I", select **IA 770 INTUITY AUDIX Messaging Application**.
3. Click on **Downloads**.
To download the IA770 patch software:
4. Click on **IA 770 INTUITY AUDIX Embedded Messaging Application Patches**.

5. Click on the service pack file name for this release.

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

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

Obtaining Optional language files

Optional languages are any language other than English (**us-eng** or **us-tdd**). If optional languages will be used with this IA770, you can also download the appropriate language files from the Download Web site.

1. Follow the steps as in [Obtaining an IA770 service pack file](#) on page 411.
2. At step [4](#), select **IA 770 INTUITY AUDIX Embedded Messaging Application Languages**.

Obtaining Ethernet interface IP address and subnet mask

If IA770 Integrated Messaging is to be installed, you must obtain an IP address and subnet mask to be used for the Ethernet interface for the H.323 integration. The subnet mask must be the same as that used for the media server (control network), and is entered on the Configure Server Web screen when you configure the S8300.

Completing the RFA process (Obtaining license and password file)

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

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

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

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

Note:

For an upgrade, you do not normally need to install a new authentication file (with a .pwd extension). However, if one is required, follow the same steps as with a license file.

Downloading license file and password file for an LSP

The license file of the S8300 as a Local Survivable Processor must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300, S8400, S8500, S8700, S8710, or S8720). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

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

Note:

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

To download the license and password files to your laptop



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

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and password files (for example, C:\licenses).
2. Access the Internet from your laptop and go to Remote Feature Activation web site, rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and password files for the customer.
4. Check that the license and password files are complete.
You might need to add the serial number of the customer's G700.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and password files to your laptop.

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

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

Note:

Business Partners call 800-295-0099. ART is available only to Avaya associates.

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

Note:

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

To run the ART

1. Access the ART web site on your laptop at <http://art.dr.avaya.com>.
2. Select **Administer S8x00 Server products for installation script**.
 - a. Log in.
 - b. Enter the customer information.
 - c. Select **Installation Script**.
 - d. Click **Start Installation script & IP Addr Admin**.

A script file is created and downloaded or emailed to you.

3. You can use the installation script to set up an IP address and other alarming parameters automatically.

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

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

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

Install the S8300

Inserting the S8300

To insert the S8300

**CAUTION:**

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

1. Connect the DVD/CD-ROM drive to the S8300 with the following steps:

Note:

You must do this *before* you completely seat the media server in the slot.

- a. Connect the USB cable into one of the USB ports on the faceplate of the S8300.
- b. Connect the other end of the USB cable to the CD-ROM or DVD/CD-RW drive.
- c. If you are using an Addonics DVD/CD-RW drive, connect the power cord to the drive and an electrical outlet.

Note:

The TEAC drive and S8300/S8400 DVD/CD-RW drive get their power from the server over the USB connection.

- d. If you are using an Addonics DVD drive, set the power source switch on the side to **EXT**, *not* **USB**.
- e. If you are using an S8300/S8400 DVD/CD-RW drive, set the on/off switch to **On**.

Be sure to set the S8300/S8400 drive to **Off** when not in use.

2. Insert the Communication Manager Software Distribution CD in the drive.

**CAUTION:**

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

3. For the S8300B circuit pack only, the LED module (above slot V1) must also be removed or inserted together with the S8300. Do the following:
 - Disengage the LED module and remove it from the G700.
 - Insert both the LED panel and S8300B circuit pack about 1/3 of the way into the guides (the guides are in slot V1 for the S8300 and above slot V1 for the LED panel).

- Push both circuit packs (together) back into the guides, gently and firmly, until the front of each circuit pack aligns with the front of the G700.

For the S8300C circuit pack only, push the module back into the slot V1 guide until the front of the S8300 module aligns with the front faceplate of the G700.

4. Secure the S8300 faceplate with the thumb screws.

Tighten the thumb screws with a screw driver.

Note:

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

5. Power up the G700 by plugging in the power cord.
6. Connect the laptop to the Services port on the faceplate of the S8300.

Installing Communication Manager Software

Note:

You cannot use the SSH protocol to access the hard drive on an S8300 Media Server that has never been installed.

Setting telnet parameters

The Microsoft telnet application may be set to send a carriage return (CR) and line feed (LF) each time you press **Enter**. The installation program interprets this as two key presses. You need to correct this before you telnet to the server.

Note:

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

To set telnet parameters

1. Click **Start > Run** to open the Run dialog box.
2. Type `telnet` and press **Enter** to open a Microsoft Telnet session.
3. Type `unset crlf` and press **Enter**.
4. Type `display` and press **Enter** to confirm that `Sending only CR` is set.
5. Close the window by clicking on the **X** in the upper-right corner.

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

Remastering the hard drive and installing the software

To do before you start the upgrade

1. Verify that the S8300 is inserted in slot V1.
2. Verify good AC power connections to the G700.
3. Avaya recommends using a UPS backup for media servers.
If a UPS is present, make sure the G700 is plugged into the UPS.
4. Verify that all Ethernet connections are secure, to ensure the file transfer process is not interrupted.

To begin the upgrade

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.

The first RP screen appears.

The first RP screen



Tip:

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

Note:

At this point, the installation script looks for the software CD on the DVD/CD drive connected to the USB port. If the DVD/CD drive was not attached to a USB port when the S8300 booted, you will not see any activity on the screen. In this case, perform the following steps:

- Press the Shut Down button on the S8300 Media Server.
- When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port and reseal the S8300 in its slot.

3. Select **Install** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen



4. Select the appropriate release version (if more than one) then select **OK** and press **Enter**.

The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen



5. Select **Yes** if you want to install IA770 concurrently with Communication Manager. Select **No** if you do not. Then press **Enter**.

Note:

If you do not install IA770 concurrently with Communication Manager at this time, and decide later to install it, you will have to upgrade Communication Manager again (even to the same release). For the upgrade, you use the Manage Software screen on the Maintenance Web interface, and select **Yes** at this screen for IA770 installation.

At this point, the following processes are initiated:

- a. The S8300 hard drive and internal Compact Flash are partitioned and reformatted.
- b. The Linux operating system is installed.
- c. Once the drive is properly configured, the program begins installing Communication Manager software and reports the progress.

Communication Manager installation progress

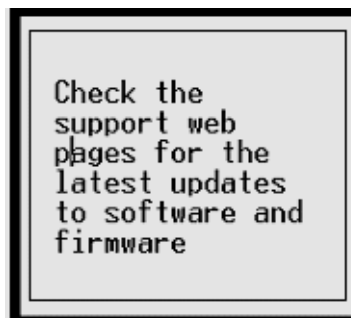
```

21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.69-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktmp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popd-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm

```

These processes take about 30 minutes. When the media server is ready to reboot, the CD drive door opens and the following screen flashes for about 5 seconds. If selected, the IA770 software is installed along with the Communication Manager software.

Software and firmware update reminder



When the installation is complete, the system reboots automatically and the telnet connection is lost. The reboot takes 1–3 minutes without the IA770 application and 3-6 minutes if the IA770 is present.

6. Click **Start > Run** to open the **Run** dialog box on your laptop.
7. Type `ping -t 192.11.13.6` and press **Enter**.
8. Wait for the reply.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See [Laptop configuration for direct connection to the services port](#) on page 42.

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

- [Accessing the server's command line interface with SSH](#) on page 55
- [Logging in to the S8300 Web Interface from your laptop](#) on page 57

Note:

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

See [About connection and login methods](#) on page 41 for details on how physically to connect and log into the G700.

Verifying Software Version

Note:

Since the system is now running a new software release, you must login with the *initial craft ID and password*. (You cannot use **dadmin** at this point.)

To verify the software version:

1. Log in to the Maintenance Web Interface.
2. Under Server, click **Software Version**.
3. Verify that the media server is running Release 4.0 software.

The **Report as:** string should show **R014x.00** at the beginning of the string. For example, **R014x.00.0.728.0**.

 Tip:

Normally, you would need to use the Make Upgrade Permanent function on the Web Interface at this point. However, this is not necessary for this upgrade because there is no previous software version in the alternate partition.

Copying Files to the S8300 hard drive

During reformatting of the hard drive, a new directory, */var/home/ftp/pub*, was created.

You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Post-upgrade software service pack
- License file
- Avaya authentication file
- New firmware files
- Security files
- IA770 service packs or RFUs

To copy files to the S8300 hard drive

1. In the Maintenance Web Interface, under **Miscellaneous**, click **Download Files**.

Note:

Since the system is now running a new software release, you must login with the *initial craft ID and password*. (You cannot use *dadmin* at this point.)

Download Files screen

Download Files

The Download Files Web page lets you download files to the media server.

☒ File(s) to download from the machine I'm using to connect to the server

☐ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

☐ Install this file on the local server

**If the above box is checked, you may specify only one file for downloading.

2. Select "Files to download from the machine I'm using to connect to the server" and browse to each file you want to copy to the S8300. Leave the "Install this file on the local server" checkbox **unchecked**.

If you need to download an IP Telephone firmware file, download this file last with the "Install this file on the local server" checkbox **checked**.

Note:

To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to `pub` after starting ftp and logging in; that is, type `cd pub`.

3. Click on **Download** to copy the files to the S8300. The transfer is complete when you see the message,

Files have been successfully uploaded to the server



Important:

Remove the Communication Manager software distribution CD from the CD drive.

Downloading optional language files, if needed

If the optional language files are needed, copy the files from the language CD to `/var/home/ftp/pub`.

To download optional language files

1. Insert the optional language CD in your laptop's CD-ROM drive.
2. On the Maintenance Web Interface, under Miscellaneous, select **Download Files**.
3. Select the **Files to download from the machine I'm using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click the **Download** button.

When the transfer is complete, the message

Files have been successfully downloaded to the server

is displayed.

6. If more than four optional language files need to be downloaded, repeat this procedure.

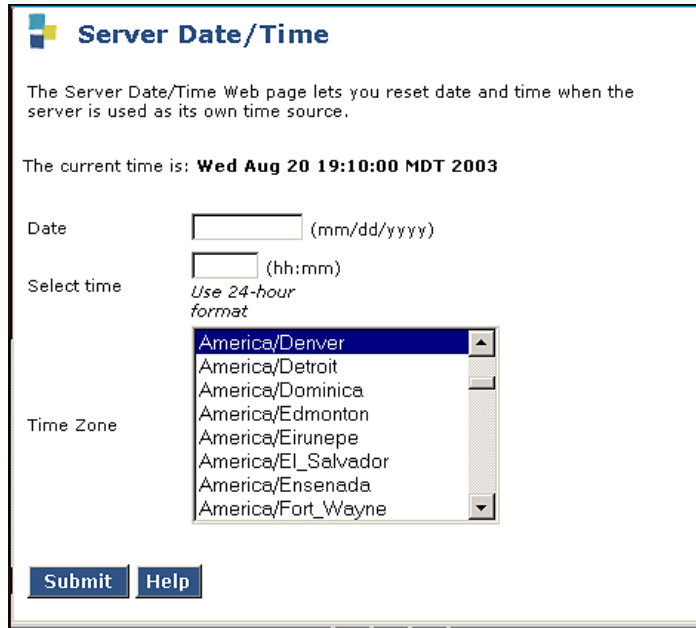
Copies of the optional language files are now in the `/var/home/ftp/pub` directory and will be automatically installed during the upgrade process.

Verifying the Time, Date, and Time Zone

To verify the Time, Date, and Time Zone:

1. Under Server click **Server Date/Time**.

Server Date/Time Window



2. Verify or set the media server's time close enough to the NTS's time, date, and time zone that synchronization can occur (within about 5 minutes).

! CAUTION:

If you are installing an LSP, you must set the time of the LSP to the same time zone as the primary controller even if the LSP is physically located in a different time zone.

Creating a super-user login, if necessary, for R4.0 or higher

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages. Use the following steps only if you are starting from Release 4.0 software or later:

Note:

A craft level login can create a super-user login in Release 4.0 or later.

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

To create a login:

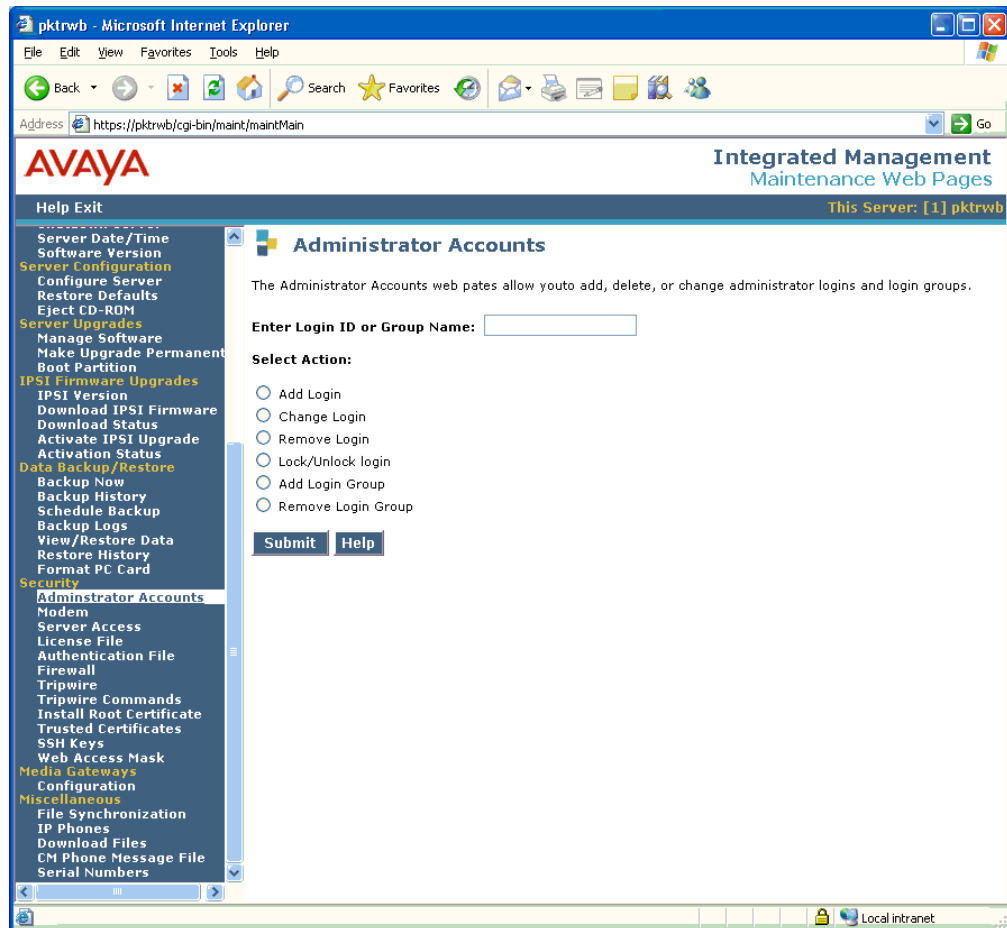
1. Ask a customer representative for a login name and password that the customer would like for the superuser login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Note:

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

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



3. Type the login name in the **Enter Login ID or Group Name** field.

4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The top header includes the Avaya logo and the title 'Integrated Management Maintenance Web Pages'. Below the header, there is a navigation menu on the left with categories like 'Server Upgrades', 'IPSI Firmware Upgrades', 'Data Backup/Restore', and 'Security'. The main content area displays the 'Administrator Logins -- Add Login' form. The form includes fields for 'Login ID' (set to 'randy'), 'login group' (set to 'susers'), 'additional groups' (set to 'prof18'), 'allow Linux shell access' (unchecked), 'lock this account' (unchecked), 'date (YYYY-MM-DD) on which account is disabled (blank to ignore)' (empty), 'select type of authentication' (radio buttons for 'password' and 'ASG', with 'password' selected), 'enter key or password' (empty), 're-enter key or password' (empty), 'force password/key change on first login' (radio buttons for 'yes' and 'no', with 'no' selected), 'maximum Number of days a password may be used (PASS_MAX_DAYS):' (set to 90), 'minimum number of days allowed between password changes (PASS_MIN_DAYS):' (set to 90), 'minimum acceptable password length (PASS_MIN_LEN):' (set to 8), 'number of days warning given before a password expires (PASS_WARN_AGE):' (empty), and 'days after password expires to lock account (0=immediate)' (empty). At the bottom of the form are 'Add' and 'Help' buttons. The status bar at the bottom shows 'Done' and 'Internet' connectivity.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

10. Complete the following fields:

- enter a challenge key or password
- re-enter challenge key or password
- force password/key change on first login

Note:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

- a. Log in with `telnet` or `ssh`.
- b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If upgrading an LSP, synchronize translations from the primary controller

If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

1. Log in with `telnet` or `ssh`.
2. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

Configuring the S8300

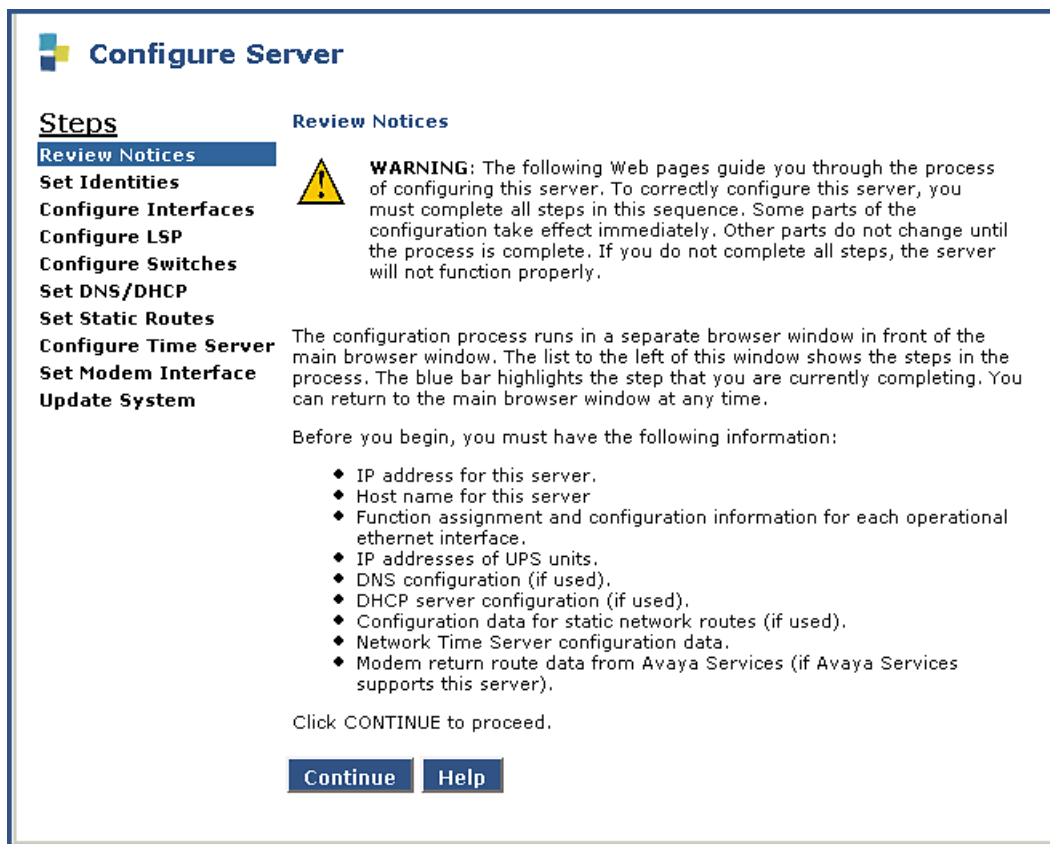
To configure the S8300 server using the Maintenance Web Interface

 CAUTION:

For a new installation, be sure you have set the time and timezone before proceeding. Failure to do so may cause network problems later.

1. On the S8300 Web page main menu, click on **Configure Server** under Server Configuration and Upgrade. The system displays the **Configure Server** screen.

Configure Server Screen



The screenshot shows the 'Configure Server' web interface. On the left is a 'Steps' sidebar with a blue bar highlighting 'Review Notices'. The sidebar lists: Review Notices, Set Identities, Configure Interfaces, Configure LSP, Configure Switches, Set DNS/DHCP, Set Static Routes, Configure Time Server, Set Modem Interface, and Update System. The main area has a 'Review Notices' section with a warning icon and text: 'WARNING: The following Web pages guide you through the process of configuring this server. To correctly configure this server, you must complete all steps in this sequence. Some parts of the configuration take effect immediately. Other parts do not change until the process is complete. If you do not complete all steps, the server will not function properly.' Below this is explanatory text about the configuration process running in a separate browser window. A list of required information is provided: IP address, host name, ethernet interface configuration, UPS unit IP addresses, DNS, DHCP, static routes, network time server data, and modem return route data. At the bottom, it says 'Click CONTINUE to proceed.' and has 'Continue' and 'Help' buttons.

2. Click **Continue**.

The system displays the **Back Up Data Notice** screen. Do one of the following options:

- For a new installation, a backup at this point is unnecessary. Perform a backup after the installation.
- For an upgrade, perform the backup, as described in [To back up the system to compact flash media \(S8300C Media Server only\)](#) on page 492.

3. Click **Continue**.

The **Select Method** screen appears.

Select Method Screen

Configure Server

Steps

- Review Notices
- Set Identities
- Configure Interfaces
- Configure LSP
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface
- Update System

Specify how you want to use this wizard

☒ Configure all services using the wizard

☐ Configure individual services

Click CONTINUE to proceed.

Continue **Help**

4. Click **Configure all services using the wizard**.

With this option, the wizard guides you through the screens to configure all of the IP services.

Note:

This option is for the built-in Web Interface configuration wizard, *not* the Avaya Installation Wizard (IW).

If you are upgrading an existing system, you may also click **Configure individual services**. This method is useful after an initial configuration has been completed and one or more services need to be changed.

5. Click **Continue**.

The **Set Identities** screen appears.

Set Identities Screen

Configure Individual IP Services

- Review Notices
- Set Identities**
- Configure Interfaces
- Configure LSP
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface

Configure Server

Set Identities

The host name of each server must be unique.

Select NIC Usage

Host Name

The following functions are assigned to the ethernet ports. Physical connections to the Ethernet ports must match these settings.

- 1. Services Port: Ethernet 0
- 2. Control Network: Ethernet 1

Click CONTINUE to proceed.

6. Enter the host name for this server in the **Host Name** field (see your planning forms).

The host name uniquely identifies this server.



CAUTION:

If the S8300 on the G700 is hosting an IA 770 INTUITY AUDIX Messaging Application *with Digital Networking*, the name *must* be 10 characters or less.

Note:

The screen also lists the current physical cabling to the server. For example, the Services laptop is connected to Ethernet interface 0. Ethernet functions are fixed on the S8300 media server and cannot be changed.

7. Click **Continue**.

The **Configure Ethernet Interfaces** screen appears.

Configure Ethernet Interfaces Screen

The screenshot shows a window titled "Configure Server" with a sidebar on the left and a main configuration area on the right. The sidebar, titled "Configure Individual IP Services", lists the following options: Review Notices, Set Identities, Configure Interfaces (which is highlighted), Configure LSP, Configure Switches, Set DNS/DHCP, Set Static Routes, Configure Time Server, and Set Modem Interface. The main area is titled "Configure Interfaces" and contains two sections: "Ethernet 0: Laptop" and "Ethernet 1: Control Network".

Ethernet 0: Laptop

IP address	192.11.13.6
Subnet mask	255.255.255.252

Ethernet 1: Control Network

IP address server1 (redtail)	135.9.80.70
Gateway	135.9.80.254
Subnet mask	255.255.255.0
Speed (Current speed : 100 Megabit full duplex)	AUTO SENSE

Integrated Messaging

IP address server1 (redtail)	135.9.80.180

Click CHANGE to change values.

At the bottom of the main area are three buttons: "Change", "Close Window", and "Help". The window's taskbar at the bottom shows a "Done" button and a "Local intranet" icon.

8. Use your planning forms to complete the fields for the:

- **Ethernet 1: Control Network**

- **IP Address server1 (hostname)** assigned to the S8300 Media Server. Check your planning forms.
- **Gateway** with the IP address of the default gateway of the subnet.
- **Subnet mask** with the value of the subnet mask of the hosting subnet.
- **Speed** which should be set to Auto Sense.

- **Integrated Messaging (if messaging software was installed earlier)**

- **IP Address server1 (hostname)** assigned to Integrated Messaging. Check your planning forms.

 CAUTION:

Do not guess on the addresses on this screen. If you enter the wrong addresses, Integrated Messaging will not be installed, service will be disrupted across the customer's network and may be difficult to correct.

9. Click **Continue**.

The **Configure Local Survivable Processor** screen appears.

Configure Local Survivable Processor Screen

Configure Server

Steps

- Review Notices
- Set Identities
- Configure Interfaces
- Configure LSP**
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface
- Update System

Configure LSP

WARNING: Changing the role of this server will **wipe out** any **translations** residing on this server and will cause a **CommunicaMgr** reset.

This page alone is not enough to completely change the role of this server. The appropriate **license file** will still need to be downloaded and installed.

☒ This is NOT a local survivable processor.
☐ This is a local survivable processor(LSP)

Note: The following information is entered only if the machine is a LSP

Component	IP Address	IP Address Duplicate Server*
Registration address at the main server (CLAN or PE Address)		
File Synchronization address at the main cluster (PE Address)		
File Synchronization address at the alternate** main cluster (PE Address)		

* only if servers are duplicated
** if used

Configure Memory

☒ Standard
☐ Extra Large

Click **CONTINUE** to proceed.

Continue **Help**

10. Select one of the following options:

- This is NOT a local survivable processor.
- This is a local survivable processor (LSP).

11. If you clicked the LSP option and the primary controller is an S8500 or S8700-series Media Server, complete the additional fields as follows:

- In the **Registration address at the main server** field, enter the IP address of a server's NIC connected to a LAN to which the LSP or ESS server is also connected. The IP address is used by the LSP or ESS server to register with the main server. In a new installation, where the LSP or the ESS server has not received the initial translation download from the main server, this address will be the only address that the LSP or the ESS server can use to register with the main server.
- **File synchronization address of the main cluster:** Enter the IP address of a server's NIC connected to a LAN to which the LSP or the ESS server is also connected. The ESS server or the LSP must be able to ping to the address. Consideration should be given to

which interface you want the file sync to use. Avaya recommends the use of the customer LAN for file sync.

Note:

The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the S8500 or S8700-series. For information on how to upgrade the firmware on the S8500 or S8700-series, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Media Servers and Gateways*, 03-300412.

12. If you clicked the LSP option and the primary controller is an S8300 or S8400 Media Server, simply enter the IP address of the S8300 server.
13. Click **Continue**.

The **Ethernet Adjuncts** screen appears.

Ethernet Adjuncts Screen

14. In the **Number of UPS Units** field, select the number of Uninterruptible Power Supplies (UPS) units connected to the S8300 Media Server.
This number is usually **0** or **1**.
15. If you enter **1** in the **Number of UPS Units** field, enter its IP address in the **UPS 1 IP Address** field.
The system will use this address to trap power loss signals from the UPS.
16. (Optional) If you enter **1** in the **Number of UPS Units** field, enter the SNMP community strings for the UPS in the **SNMP GET** and **SET** fields.

17. Click **Continue**.

The **External DNS Server Configuration** screen appears.

Most corporate networks have one or more domain name service (DNS) servers that associate an IP address with a device's name. When the DNS is administered with the S8300 Media Server name, you will be able to access the S8300 server by name as well as IP address over the corporate network.



CAUTION:

If you configure an external DNS server, the DNS will be an extra device that, if not working properly, can cause delays in S8300 access.

External DNS Server Configuration Screen

Configure Individual IP Services

- Review Notices
- Set Identities
- Configure Interfaces
- Configure LSP
- Configure Switches
- Set DNS/DHCP**
- Set Static Routes
- Configure Time Server
- Set Modem Interface

Configure Server

External DNS Server Configuration
Note: If DNS is not used, leave these fields blank.

Name Servers

IP Address 1

IP Address 2

IP Address 3

DNS Domain

Search Domain 1

Search Domain 2

Search Domain 3

Search Domain 4

Search Domain 5

Click CHANGE to change values.

18. Enter the appropriate IP addresses from your planning documentation.

Complete the following fields:

- In the **Name Servers** fields, enter the IP addresses for up to 3 DNS servers on the corporate network.

The S8300 Media Server checks the DNS servers in the order in which their addresses are entered for name-to-IP address resolution.

- In the **DNS Domain** field, enter the name for the part of the network on which the DNS server(s) reside (for example, *mycompany.com*).

Internet domains are sets of addresses generally organized by location or purpose.

- In the **Search Domain** fields, **1** to **5**, enter the names of the domains that will be searched, in order, if a user enters an unqualified or incomplete name (such as a host name only without its domain).

Note:

For **Search Domain 1**, enter the *same domain name* you entered in the **DNS Domain** field above.

19. Click **Close Window**.

The **Static Network Routes** screen appears.

Static Network Routes are used only if the customer has defined additional routes for IP packets other than through the default gateway. Leave these entries blank, unless the planning documentation supplies routing information.

Set Network Routes Screen

Configure Individual IP Services

- Review Notices
- Set Identities
- Configure Interfaces
- Configure LSP
- Configure Switches
- Set DNS/DHCP
- Set Static Routes**
- Configure Time Server
- Set Modem Interface

Configure Server

Static Network Routes (Optional)

Add routes by filling in the fields. Remove routes by deleting information from the fields.

	<u>IP Address</u>	<u>Subnet Mask</u>	<u>Gateway</u>	<u>Interface</u>
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				

Click **CHANGE** to change values.

Change **Close Window** **Help**

20. Click **Continue**.

The system displays the **Network Time Server** screen.

The **Network Time Server** screen allows you to set up the Network Time Protocol (NTP) Service.

Network Time Server Screen

The screenshot shows a web-based configuration interface for a Network Time Server. On the left is a dark blue sidebar with a list of configuration options: 'Configure Individual IP Services', 'Review Notices', 'Set Identities', 'Configure Interfaces', 'Configure LSP', 'Configure Switches', 'Set DNS/DHCP', 'Set Static Routes', 'Configure Time Server' (highlighted with a yellow box), and 'Set Modem Interface'. The main content area is titled 'Configure Server' and contains the 'Network Time Server' configuration section. It includes radio buttons for 'Time of Day Synchronization': 'Disable NTP, Use Local Clock', 'Enable NTP, Use Local Clock', and 'Use these Network Time Servers:'. The third option is selected. Below it are fields for 'Primary', 'Secondary', and 'Tertiary' servers, each with a 'Trusted Key' field. The 'Primary' server field contains 'ntp2a.dr.avaya.com'. There are also radio buttons for 'Multicast Client Support' (Yes/No), with 'No' selected. At the bottom, there are radio buttons for installing a keys file from a specific path or not installing one, with 'Do not install a new keys file' selected. A note says 'Click CHANGE to change values.' and there are three buttons: 'Change', 'Close Window', and 'Help'.

Configure Individual IP Services

- Review Notices
- Set Identities
- Configure Interfaces
- Configure LSP
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server**
- Set Modem Interface

Configure Server

Network Time Server

Time of Day Synchronization

☐ Disable NTP, Use Local Clock

☐ Enable NTP, Use Local Clock

☒ Use these Network Time Servers:

Primary: (IP Address or DNS Name)

Trusted Key: (Leave blank if not used)

Secondary:

Trusted Key: (Leave blank if not used)

Tertiary:

Trusted Key: (Leave blank if not used)

Multicast Client Support: ☐ Yes ☒ No

Additional Trusted Keys:

Requested Key:

Control Key:

☐ Install keys file from /var/home/ftp/pub/keys.install

☒ Do not install a new keys file

Click CHANGE to change values.

Make the following choices, according to the planning documentation:

- Choose **Disable NTP** if the user does not want the Network Time Protocol to run on the S8300 Media Server.

Select this option to disable Network Time Protocol (NTP) and use the media server's own clock as a time source. You typically choose this option if this is the only media server in the configuration and it will not be synchronized with an external time source.

- Choose **Enable NTP** if the S8300 Media Server will be the primary NTP server.

Optionally, you can provide the address of the survivable S8300 Media Server in the local survivable configuration. Select this option to enable NTP and use the media server's own clock as a time source. You typically choose this option if there is more than one media server in the configuration (for example, this or another media server may be acting as an LSP standby unit), and an external time source is not available to provide

synchronization between the units. Select this option to enable NTP and use its own clock as a time source. You need to set up the time clock with Set Server Time/Timezone option. You need to set the server clock using the Set Server Time / Timezone screen. You can do this now, then return to the Configure Server window.

- Choose **Use these Network Time Servers** to enter up to three time servers.

Select this option to enable NTP and be synchronized with an external time source on the corporate network.

21. If you did not select **Use these Network Time Servers** in the previous step, click **Continue** and go to the next step.

If you selected **Use these Network Time Servers** in the previous step, complete the following fields:

Specify up to three network time servers by IP address or DNS name in the order in which you want the S8300 Media Server to check them. You should always specify at least two.

- **Primary** — Enter an IP address or DNS name.

If a trusted key is required, enter a valid key number in the **Trusted Key** field.

- **Secondary** — Enter an IP address or DNS name.

If a trusted key is required, enter a valid key number in the **Trusted Key** field.

- **Tertiary** — Enter an IP address or DNS name.

If a trusted key is required, enter a valid key number in the **Trusted Key** field.

- **Multicast Client Support** — Select **Yes** if the NTS routinely broadcasts its timing messages to multiple clients.

Select **No** if the S8300 Media Server is to poll (directly request the time from) the NTS.

- **Additional trusted keys** (optional) — If you want to encrypt the messages between an NTS and the S8300 Media Server, list the valid key numbers, up to 3, provided by your LAN administrator on the pre-installation worksheet.

Trusted keys function like a checksum to make sure the time packets are valid. Use a blank space as a delimiter if there is more than one key (for example, 2 3 6 to specify valid keys 2, 3, and 6). These numbers are associated with encryption codes in a "keys" file.

- **Request key** — Enter a key to send a remote query request.

Only 1 key is allowed in this field.

- **Control key** — Enter a key to query and request changes to an NTS.

Only 1 key is allowed in this field.

22. If you have a file named *keys.install* to allow the media server to communicate with the NTS, select **Install keys from var/home/ftp/keys.install**.

If you do not have a *keys.install* file, select **Do not install a new keys file**.

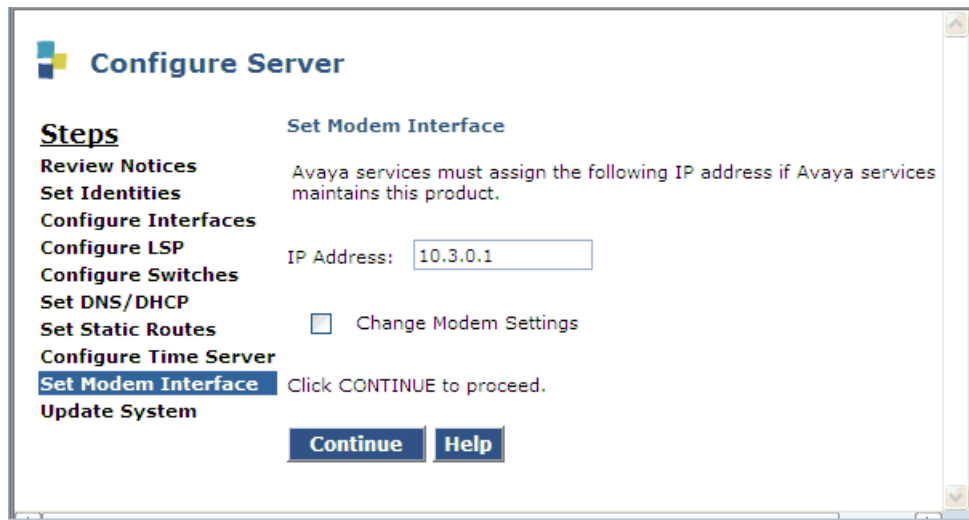
Note:

If you have a *keys.install* file, upload or create it now, if possible. See [Providing the keys.install File \(If Necessary\)](#) on page 440. If you upload the keys file later, you have to run the Web Interface Configure Server wizard again to have the system recognize it.

Click **Continue**.

23. At the next screen, **Set Modem Interface**, you can set up the Modem Interface IP Address for Avaya-provided service.

Set Modem Interface Screen



Configure Server

Steps

- Review Notices
- Set Identities
- Configure Interfaces
- Configure LSP
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface**
- Update System

Set Modem Interface

Avaya services must assign the following IP address if Avaya services maintains this product.

IP Address:

☐ Change Modem Settings

Click CONTINUE to proceed.

Continue **Help**

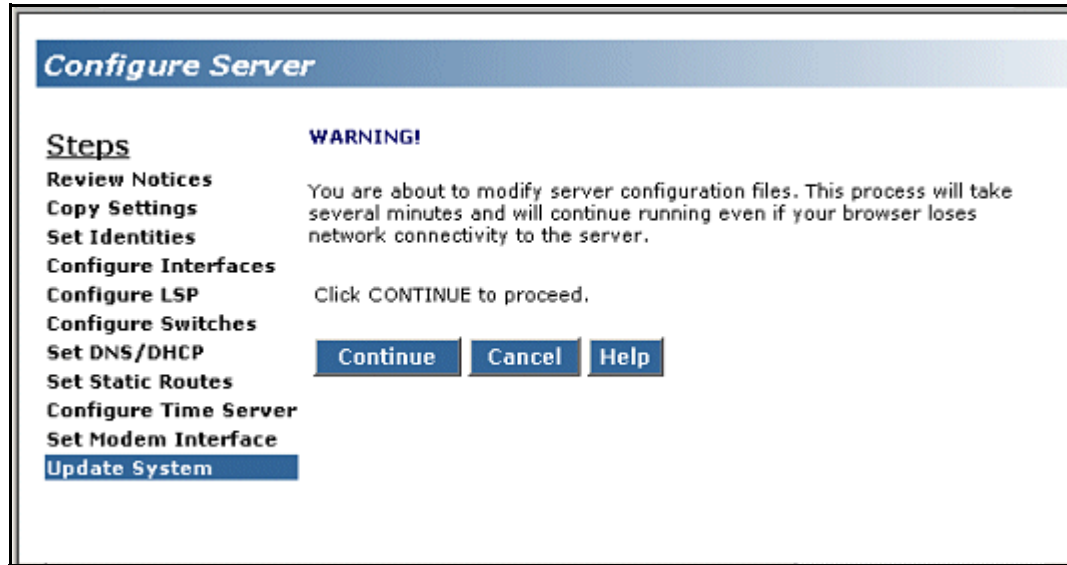
Note:

The Modem IP Address for the Avaya INADS alarming is assigned by the ART tool. You should have obtained this address when you performed [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 413.

Click **Continue**.

The next **Warning** screen indicates that the data entry process has concluded and that the system is ready to be configured.

Warning Screen

**Note:**

This is the final step in configuring the system. When you click **Continue**, all the configuration information will be written to disk and implemented. This step normally completes in about 5 minutes.

This is your last chance to cancel or correct the configuration.

24. To check, or possibly change, something you entered on a previous screen, use your browser's **Back** button to page back through the **Configure Server** screens.
25. Check or change the items in question.
26. Click the **Continue** button to move forward again, whether you change anything or not. If you don't do this, information in the wizard may not be processed correctly.

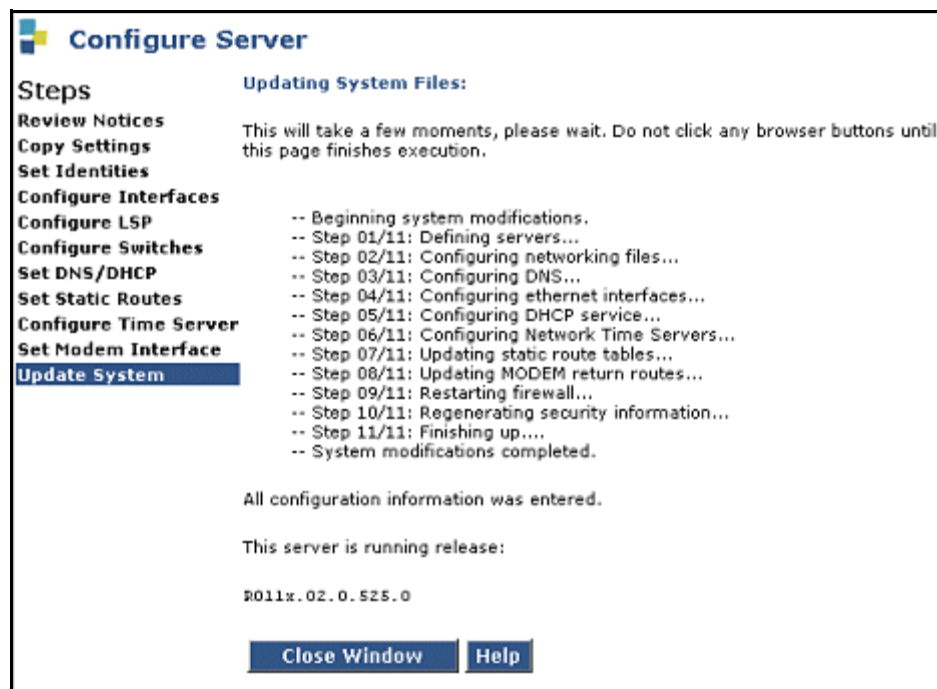
Note:

For any configuration, it is always safe to **Cancel** the configuration, and run the Configure Server screens of the Web Interface again later from the beginning. You might use this option if you are checking or modifying settings on a server that has already been configured, and there is not a large amount of new information to enter.

27. On the **Update System** screen, if you are satisfied that everything is set correctly, click **Continue**.

You can watch the progress of the configuration at the **Updating System Files** screen. If the configuration status displays stops updating at some point and the screen appears to freeze, you may have lost contact with the server. In this case, the configuration process will continue and you can log back on and pick up where left off.

Updating System Files Screen



When the process is complete, you will receive a notification.

28. Click **Close Window** and continue the configuration of the G700 Media Gateway on the command line interface.

Providing the keys.install File (If Necessary)

Use this procedure only if you selected one of the customer-provided keys options in the previous procedure.

If encryption between the NTS and S8300 Media Server is to be used for additional security, you *must* provide a keys.install file that specifies for each key:

- The key number
- The encryption type
- The key code

If the keys file is short, the network administrator can create one now during configuration if needed:

To create the key file

1. On a directly connected laptop or other computer, create a flat-text file named *keys.install*, with the correct keys information using any ASCII application (for example, Notepad).
2. Upload the *keys.install* file using the **Upload Files to Server** screen as described earlier.
3. When finished, click on the **Configure Server** wizard window to resume server configuration.

The keys file can be loaded in one of the following two ways. If a *keys.install* file was previously created on or downloaded to the services laptop or another computer on the network, it can be installed now, as follows:

To upload the keys file

1. In the main menu under **Miscellaneous**, click the **Upload Files to Server** link.
2. Locate the *keys.install* file on your computer or network, then click **Load File**.
The file is uploaded to the media server's FTP directory.
3. When finished, click on the **Configure Server** wizard window to resume server configuration.

Longer files may be transferred from the network time server to the S8300 Media Server as follows:

To download or copy the keys file

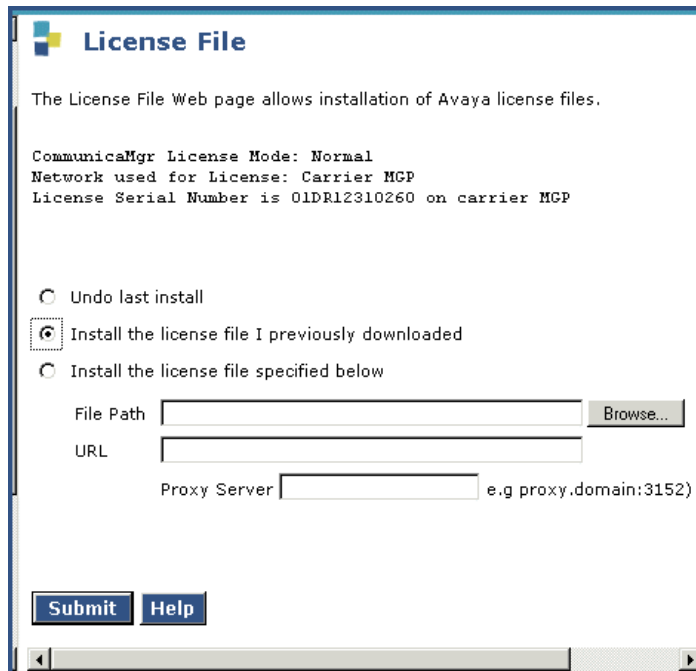
1. Using either the **Download Files to Server** screen or the Transfer files using an FTP procedure to access the keys file listed on your pre installation worksheet.
In both cases, the file is transferred to the media server's FTP directory.
2. When finished, click on the **Configure Server** wizard window to resume server configuration.
3. After the *keys.install* file is uploaded, select the location where it resides, usually in the **/var/home/ftp** subdirectory. (Services personnel may direct you to use the **/tmp** directory.)
4. If a keys file is not used, or if the correct *keys.install* file is already installed, select the option not to install a new keys file.

Installing the license and authentication files

To install the license and authentication files

1. Under Security, select **License File**.
The **License File** screen appears.

License File Screen



The License File Web page allows installation of Avaya license files.

CommunicationsMgr License Mode: Normal
Network used for License: Carrier MGP
License Serial Number is 01DR12310260 on carrier MGP

☐ Undo last install
☒ Install the license file I previously downloaded
☐ Install the license file specified below

File Path
URL
Proxy Server (e.g. proxy.domain:3152)

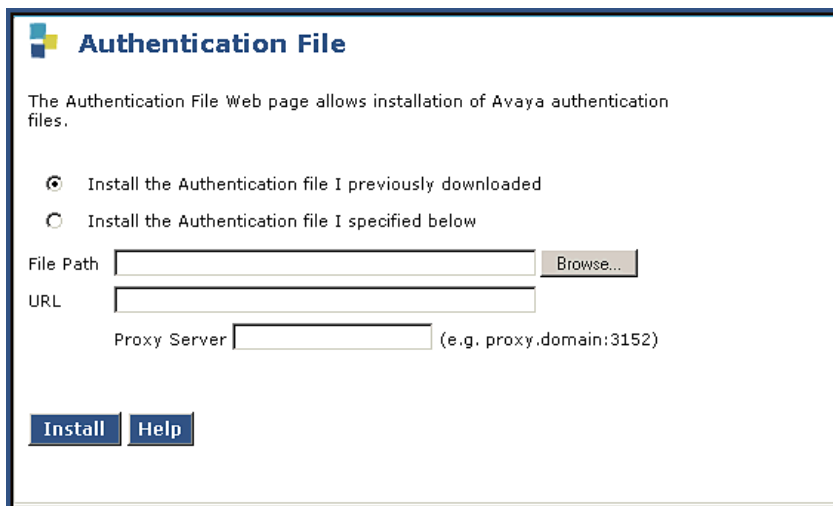
2. Select **Install the license file I previously downloaded** and click **Submit**.

The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.

The **Authentication File** screen appears.

Install Authentication Screen



The Authentication File Web page allows installation of Avaya authentication files.

☒ Install the Authentication file I previously downloaded
☐ Install the Authentication file I specified below

File Path
URL
Proxy Server (e.g. proxy.domain:3152)

4. Select "Install the Authentication file I previously downloaded" and click **Install**.

The system tells you the authentication is installed successfully

If the authentication file does not install, you may need to add a super-user login first. See [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 424.

If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`
3. Type `start -ca`

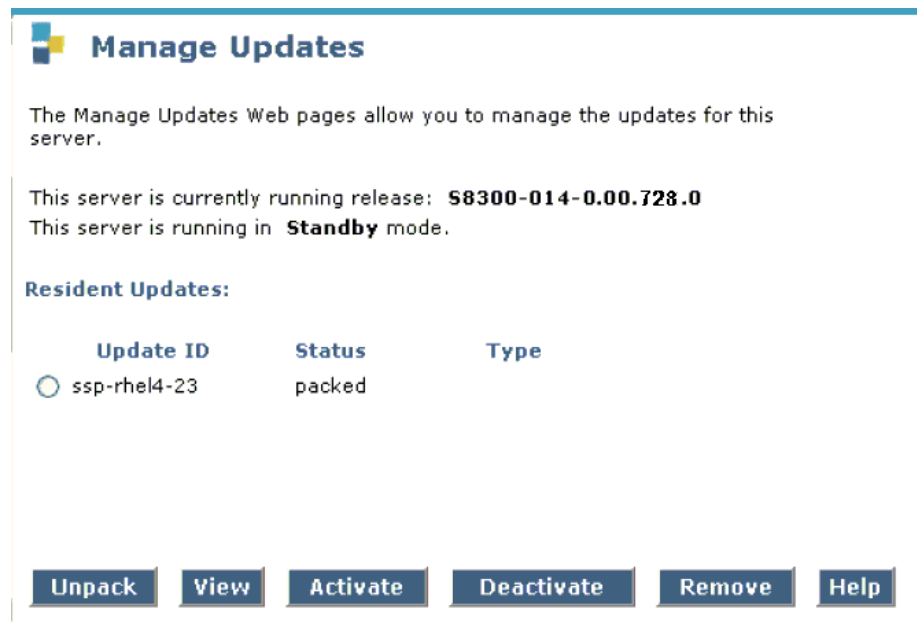
Installing security files and Communication Manager service packs, if any

To install security files and/or service packs

1. Under Server Upgrades, select **Manage Updates**.

The **Manage Updates** screen appears.

Manage Updates Screen



2. Do one or both of the following:
 - a. If there are earlier versions of files that you are updating, select those versions and click **Deactivate**.

The screen shows the status of the deactivation.
 - b. If a file you want to activate shows **packed** in the **Status** column, select that file and click **Unpack**.

The screen shows the status of the unpacking.
3. Check the **Type** column for the file you want to activate. Tell the customer that the system will reboot if the file type is **cold**. The customer may want to wait to install this security update.
4. Select the file you want to activate and click **Activate**.

The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

Saving Translations

Note:

If the S8300 you are upgrading is an **LSP**, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session. and log in as *craft* (or *dadmin*).
2. If the S8300 you are installing is a primary controller, at the SAT prompt, type **save translation** and press **Enter**.
3. If the S8300 you are installing is an LSP, then on the primary controller, type **save translation lsp** and press **Enter**. This command distribute saved translations out to the LSPs.

When the save is finished, the system displays the message,

Command successfully completed.

The system automatically performs a reset system 4. If you are upgrading an LSP, you are logged out.

Configure the G700 Media Gateway

This section describes the procedures for assigning IP addresses to the G700 components and for assigning IP routing.

The section contains:

- [Assigning IP Addresses of the G700 Media Gateway Components](#)
- [Setting up the Controller List for the G700](#)
- [Configuring an X330 Expansion Module \(If Necessary\)](#)

Assigning IP Addresses of the G700 Media Gateway Components

This section describes how to assign the IP addresses and IP routes to the G700 Media Gateway and its components. The IP addresses should be available to you on the IP Addressing Planning Form. The command arguments you will be supplying include:

- VLAN — Virtual Local Area Network: a defined network segment that allows users on that segment to have priority services in sharing information with each other.

If the network is not using VLANs, the VLAN should be 1. Otherwise, use the VLAN numbers indicated in your planning forms. The G700 Media Gateway should be assigned the same VLAN as the VLAN to which the Ethernet ports are connected. The P330 stack processor might or might not be assigned to the customer's network management VLAN.

- IP address — the unique identifier assigned to an entity on the customer LAN.
- Netmask — the subnet mask for the customer's LAN segment.
- Destination — distant networks to which the IP route command needs to send packets. Usually generalized to 0.0.0.0 for networks other than the local segment.
- default gateway — the gateway the ip route command specifies to get to the distant networks.

This section contains the following procedures:

- [To access the P330 stack processor](#)
- [To assign the IP address to the P330 stack processor](#)
- [To establish IP routing for the stack](#)
- [To check the serial number of the G700 media gateway processor](#)
- [To assign the IP address to the G700 media gateway processor](#)

- [To assign the default IP route to the G700 media gateway](#)
- [To assign IP addresses to the VoIP resources](#)
- [Checking for IP connections](#)

To access the P330 stack processor

1. Set up a direct connection to the G700 Console (serial) port and access the P330 stack processor using Hyperterminal (or similar terminal emulation application).
2. Login as *root*.

To assign the IP address to the P330 stack processor

1. At the **P330-1(super)#** prompt, type `nvrw init` to initialize the default values of the media gateway processor.

This command ensures that any existing configuration information is cleared so you can enter the IP address and IP route information.

The system prompts you to verify that you want to erase the configuration.

2. Answer the prompt by typing `y(es)`.

The process re-initializes the G700 software back to factory defaults so new IP addresses can be stored correctly in the software. It also clears all configuration and administration on the G700 Media Gateway.

The G700 Media Gateway re-initializes.

3. Type `configure` to change to configuration mode.

4. At the **P330-1(configure)#** prompt, type `set interface inband <vlan> <ip_address> <netmask>` to assign an IP address to the P330 stack processor.

`<vlan>` is the vlan number, usually 1, to be established on the S8300 for the G700 Media Gateways. The `<ip_address> <netmask>` is the assigned address and subnet for the P330 stack processor.

5. Type `reset` and press **Enter** to reset the stack.

Select **Yes** at the dialog box that asks if you want to continue.

All LEDs flash. As the unit powers up, self-tests are run. When the G700 MPG or P330 stack processor has reset, login again to continue.

6. Login at the **Welcome to P330** menu.

The prompt **P330-1(super)#** appears.

7. Type `configure` to obtain the **P330-1(configure)#** prompt.

To establish IP routing for the stack

1. Type `show interface inband` to verify that the Avaya P330 stack server (Layer 2 Switching Processor) has the correct address.
2. Type `set ip route 0.0.0.0 <default-gateway>` to specify the gateway to handle addresses outside of the local subnet.

`<default-gateway>` is the IP address of the customer's default network gateway. This address should be available in the planning documentation.
3. Press **Enter** to save the destination and gateway IP addresses.
4. Type `show ip route`.

The route net and route host tables appear. Verify that the information is correct.

After you have configured the P330 stack processor, you assign an IP address to the G700 Media Gateway Processor (MGP). Your first task is to check the serial number of the MGP.

To check the serial number of the G700 media gateway processor

1. At the **P330-1(configure)#** prompt, type `session mgp`.
2. At the **MG-???-1(super)#** prompt, type `show system` to list various attributes of the G700.

The system displays a list of attributes, as shown in the following example:

Show System List for G700 Media Gateway

```

Welcome to Media Gateway Processor
FW version 25.25.0

MG-001-1(super)# show system
Uptime(d,h:m:s): 8, 21:34:15
System Name      : -- Empty --
System Location  : -- Empty --
System Contact   : -- Empty --
MAC Address      : 00-04-0D-02-06-CA
Serial No        : 01DR12310260
Model No         : G700
HW Vintage       : 01
HW Suffix        : B
FW Vintage       : 25.25.0

Media Gateway Power Supplies
VOLTAGE(V)  ACTUAL(V)  STATUS
-----
DSP Complex  3.4        3.369    OK
MGP          5.1        5.099    OK
Media Modules -48.0     -48.360  OK
VoIP DSP     1.6        1.590    OK
VoIP 8260    2.5        2.480    OK

MG-001-1(super)#

```

3. Write the serial number on your planning document.

Make sure it matches the serial number sticker on the back of the G700 Media Gateway chassis. If there is a difference, the serial number in the displayed list is correct. You will need this later.

After you have assigned an IP address to the G700 processor, telnet directly to the G700 media gateway processor and login (the login name and password are provided in the planning documentation).

To assign the IP address to the G700 media gateway processor

1. At the **MG-???-n(super)#** prompt, type **configure** to change to configuration mode.

2. Type **nvrw init** to initialize the default values of the media gateway processor.

This command ensures that any existing configuration information is cleared so you can enter the IP address and IP route information.

The system prompts you to verify that you want to erase the configuration.

3. Answer the prompt by typing **y(es)**.

This process re-initializes the G700 software back to factory defaults so new IP addresses can be stored correctly in the software. It also clears all configuration and administration on the G700 Media Gateway.

The G700 Media Gateway re-initializes.

4. At the **P330-1(configure)#** prompt, type **session mgp**.

5. At the **MG-???-1(super)#** prompt, type **configure** to change to configuration mode.

6. Type **set interface mgp <vlan> <ip_address> <netmask>** to assign an IP address to the G700 Media Gateway.

<vlan> is the vlan to be established on the customer's local network. This is usually **1**. The **<ip_address> <netmask>** is the assigned IP address and subnet for the G700 media gateway.



CAUTION:

If this G700 contains an S8300 configured as an LSP, use the VLAN administered on the primary controller.

7. At the **MG-???-n(configure)#** prompt, type **reset mgp**.

A system prompt asks to confirm the reset.

8. Select **Yes** at the dialog box that asks if you want to continue.

The G700 Media Gateway processor resets. The LEDs on the G700 Media Gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

9. At the **P330-1(configure)#** prompt, type **session mgp**.

10. At the **MG-???-1(super)#** prompt, type **configure** to reach the configuration level of the command line interface.
11. Type **show interface mgp** to verify that the G700 media gateway has the correct IP address.

To assign the default IP route to the G700 media gateway



CAUTION:

The default gateway IP routing address is *required* for Communication Manager 4.0.

1. At the **MG-???-n(configure)#** prompt, type

```
set ip route 0.0.0.0 0.0.0.0 <default_gateway>
```

to specify the gateway to handle addresses outside of the local subnet.

<default_gateway> is the IP address of the default network gateway. This address should be available in the planning documentation.
2. Type **show ip route mgp** to view the results.
3. Repeat Step 1 for additional ip routes, if needed.

Usually, only a default route is needed. Refer to your planning document.

From the G700 media gateway processor command line interface, you assign IP addresses to the VoIP resource resident on the G700 media gateway and to any installed MM760 VoIP media modules.

To assign IP addresses to the VoIP resources

1. At the **MG-???-n(configure)#** prompt, type **set interface voip <number> <ip address>**

<number> is the slot number of the VoIP media module. **v0** designates the VoIP resource resident on the G700 Media Gateway motherboard. The MM760 VoIP Media Modules are designated according the slot (for example, **v1**, **v2**, **v3**, **v4**) in which the media module has been installed.

<ip address> is the IP address of the VoIP resource.

For example: **set interface voip v0 132.236.73.3**
2. Type **show interface** to display a table of all configured interfaces, including all VoIP Media Modules.
3. Type **show voip v0** to display the VoIP resource on the motherboard.

Note:

It is not necessary to configure the VLAN, netmask, or IP routes for VoIP engines. The media gateway parameters are applied automatically.

Checking for IP connections

After you have assigned IP addresses to the P330 Stack Processor (Layer 2 Switching Processor), the G700 Media Gateway MGP, media modules, and the VoIP resources, validate the IP connections.

To run the ping command

1. At the **MG-???-1(config)#** prompt, type **ping mgp <IP_address>**

where **<IP_address>** is the address of an S8300, S8500, S8700, S8710, or S8720 Media Server, the VoIP engine, or any other functioning endpoint accessible on the customer's LAN. It is recommended to ping endpoints on both the same subnet and a different subnet.

Ping results appear on the screen, similar to the following example.

Ping MGP results

```
MG-???-1(configure)# ping mgp 135.122.49.55
PING 135.122.49.55: 56 data bytes
64 bytes from 135.122.49.55: icmp_seq=0. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=1. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=2. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=3. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=4. time=0. ms
----135.122.49.55 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

2. Check that the same number of packets transmitted were also received.

3. Type **ping voip v0 <IP_address>**

<IP_address> is the address of the G700, or any other functioning endpoint on the customer's LAN.

Ping results appear on the screen, similar to the following example.

Ping VoIP results

```
MG-???-1(configure)# ping voip v0 135.122.49.55

----135.122.49.55 PING Statistics----
5 packets transmitted, 5 packets received, 0 packet loss
round-trip(ms) min/avg/max = 0/1/0
```

Setting up the Controller List for the G700

To complete the configuration of the G700 media gateway, you need to administer a list of primary and alternate controllers. This list begins with the IP address of the primary controller. In the event that the G700 media gateway loses contact with its primary controller, it will seek to re-register with the primary controller first, then with the other controllers on this list. The other controllers are S8500 or S8700/S8710/S8720 media servers that can act as the primary controller, or S8300 media servers configured as Local Survivable Processors (LSPs).

Up to four IP addresses separated by commas can be entered to form the controller list.

To set the MGP controller list

1. At the **MG-???-n(configure)#** prompt, type the following commands to designate the primary, secondary, and LSP controllers for this G700:

- a. `clear mgc list`

- b. `set mgc list <ip_address> [,<ip_address> [,<ip_address>
[,<ip_address>]]]`

where, the first `<ip_address>` can be one of the following IP addresses:

- For an S8700-series primary controller, the IP address of a C-LAN board that is connected to the primary controller.
- For an S8400 or S8500 primary controller, the IP address of either a C-LAN board that is connected to the primary controller, or an Ethernet port, on the server itself, that has been enabled for processor Ethernet connections.
- For an S8300 primary controller, the IP address of the S8300.

The next three `<ip_address>` parameters are optional IP addresses of up to three alternate controllers. Each of the three optional controllers can be a second C-LAN connected to the primary controller (S8400, S8500, or S8700-series Media Servers), an S8300 configured as an LSP, or the port enabled as the Ethernet processor port on an S8500 configured as an LSP. The types of alternate controllers in the list depend on the G700's primary controller and the other controller devices it supports.



CAUTION:

If you need to change the mgc list, you must run `clear mgc list` before running `set mgc list` again. You can also remove a single address in the list with the command `clear mgc list <ip address>`.

[Table 29](#) describes the possible optional controllers for an S8300 and S8700/S8710/S8720 primary controller:

Table 29: Possible optional controllers for various primary controllers

If primary controller is	Then, controller IP addresses can be
S8300	First: IP address of the S8300 primary controller. Next three: one, two, or three IP addresses of S8300s configured as LSPs.
S8400, S8500 or S8700, S8710, or S8720	First: IP address of the C-LAN for the S8400, S8500, or S8700/S8710/S8720 primary controller or IP address of processor Ethernet-enabled port on S8400 or S8500. Next three: one, two, or three IP addresses of alternate C-LANs and/or LSPs.

Note:

For an S8500 or S8700/S8710/S8720 primary controller, If you enter a combination of both C-LANs and LSPs, you must list C-LANs first.

2. Type **reset mgp** at the **MG-???-n(configure)#** prompt to reset the G700 media gateway processor.

A system prompt asks you to confirm the reset.

3. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

The system ultimately returns you to the **P330-1 (configure)** prompt.

At the **P330-1(configure)#** prompt, type **session mgp**.

At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.

Note:

Because the G700 media gateway has registered with its primary controller, the prompt name has changed; for example, to **MG-001-1**.

Type **show mgc** to display the list of available servers and their IP addresses.

For example:

Show Call Controller Status Screen

```
MG-001-1(configure)# show mgc
CALL CONTROLLER STATUS
-----
Registered           : YES
Active Controller    : 135.9.71.95
H248 Link Status     : UP
H248 Link Error Code : 0x0
MGC List Management  : Static

CONFIGURED MGC HOST          DHCP SPECIFIED MGC HOST
-----
135.9.71.95                  -- Not Available --
- Not Available --          -- Not Available --
- Not Available --          -- Not Available --
- Not Available --          -- Not Available --
```

The Gateway will have registered with the primary controller, if present. If the primary controller is running and has been administered properly, the **Registered** field says YES and the **H248 Link Status** says UP. If the controller is not running, the **Registered** field says NO and the **H248 Link Status** says DOWN.

Setting the LSP Transition Points

You must set the length of time that the G700 searches, in the event of a network problem, for primary controllers (for example, additional CLAN connections) with which to register. After this search time has elapsed, the G700 will search for an LSP with which to register. You must also set the total time the G700 searches for either a primary controller and an LSP, after which the G700 resets. And finally, you must define how many primary controllers, from 1 to 4, are in the controller list you just defined.

To set LSP transition points

1. At the **MG-001-1(configure)#** prompt, type **set mgp reset-times primary-search <search-time>**

where **<search-time>** is the time in minutes that the G700 searches for a primary controller before looking for an LSP. The range is from **1** to **60**.

2. At the **MG-001-1(configure)#** prompt, type **set mgp reset-times total-search <search-time>**

where **<search-time>** is the total time in minutes that the G700 searches for both primary controllers or LSPs. The range is from **1** to **60**.

3. At the **MG-001-1(configure)#** prompt, type `set mgp reset-times transition-point <#_of_primary>`

where `<#_of_primary>` is the number of primary controllers in the controller list. If the primary controller is an S8500 or S8700/S8710/S8720, the range is from **1** to **4**. If the primary controller is an S8300, `<#_of_primary>` must be **1**.

Configuring an X330 Expansion Module (If Necessary)

User Guides and Quick Start Guides for the expansion modules are available on the Avaya Support web site:

To obtain the appropriate Avaya Support Web site document

1. Go to the Avaya Support web site: <http://avaya.com/support>.
2. In the list on under Technical Database, click on **LAN, Backbone, and Edge Access Switches**.
3. Under Wiring Closet & Distribution, click on **P330 Stackable Switching**.
4. Click on **All Documents**.
5. Select the appropriate document for the expansion module you are installing.

Install New Firmware on the G700

This section describes the manual procedures to install firmware on the G700 Media Gateway processors and media modules.

Manual upgrade procedures — G700 firmware

This section contains the following tasks:

- [Verifying the Contents of the tftpboot Directory](#)
- [Determining which firmware to install on the G700](#)
- [Installing New Firmware on the P330 Stack Processor](#)
- [Installing new firmware on the G700 Media Gateway Processor](#)
- [Installing new firmware on the media modules](#)

Verifying the Contents of the `tftpboot` Directory

Before proceeding with the G700 firmware installation, you should check the `/tftpboot` directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the `/tftpboot` directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.
2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the `/var/home/ftp/pub` directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the `pub` directory.

3. Copy the firmware files from the `pub` directory to the `/tftpboot` directory, using the S8300 Media Server command line interface.

To copy firmware files to the `/tftpboot` directory of an S8300 Media Server, do the following:

- a. Use SSH, Avaya Site Administration, or another tool to access the S8300 Media Server command line.
- b. Log in as `craft`.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to `/var/home/ftp/pub`.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the `/tftpboot` directory. To copy multiple firmware files (most firmware files have an `.fdl` suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the `/tftpboot` directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to `/tftpboot`.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

Conduct the following procedure to compare software versions running on the G700 processors and media modules with the versions in your planning documents. If the versions do not match, you need to install the new firmware for those components.

To determine if new firmware for the P330 stack processor is necessary

1. At either the **P330-1(super)#** or **P330-1(configure)#** prompt, type **dir**.

The system displays the directory list of software for the P330 stack processor.

Directory list for P300 stack processor

M#	file	ver num	file type	file location	file description
--	----	-----	-----	-----	-----
1	module-config	N/A	Running Conf	Ram	Module
	Configuration				
1	stack-config	N/A	Running Conf	Ram	Stack Configuration
1	EW_Archive	4.0.4	SW Web Image	NV-Ram	WEB Download
1	Booter_Image	3.2.5	SW BootImage	NV-Ram	Booter Image

2. Check the version number (ver num) of the EW_Archive file to see if it matches the Release Letter.

If not, you must upgrade the P330 stack processor.

3. Type **show image version**

The system displays the list of software.

Show image version List for P330 stack processor

Mod	Module-Type	Bank	Version
-----	-----	----	-----
3	Avaya G700 media gateway	A	0.0.0
3	Avaya G700 media gateway	B	4.0.17

4. Check the version number of the stack software image file in Band B to see if it matches the your planning document.

If not, you must upgrade the P330 stack processor.

To determine if new firmware is required for the MGP, VoIP module, and installed media modules

1. Type **session mgp**
2. At the **MG-001-1(super)#** prompt, type **show mg list_config**

The system displays the list of software.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (B)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

3. Refer to the list to check the FW vintage number of the G700.

In the TYPE column, find G700, then check the matching field in the FW VINTAGE column to see if it matches the vintage number in your planning forms. If not, you must install new firmware on the G700 media gateway. Also check if the release number in the FW VINTAGE column contains (A) or (B) to designate the software bank. If the list shows B, you will upgrade A. If the list shows A, you will upgrade B.

4. Refer to the VOIP FW column and row for slot V0 (same row occupied by the G700 information) to see if the number matches the VoIP firmware identified in your planning forms.

If not, you must also upgrade the G700 media gateway motherboard VoIP module.

Note:

The VoIP processor on the motherboard is upgraded using the same firmware image file as the VoIP media modules; for example, the file mm760v8.fdl is vintage #8.

5. Check the FW VINTAGE column for vintages of each of the installed media modules: MM710, MM711, MM712, MM714, MM716, MM717, MM720, MM722, and/or MM760 to see if they match the FW vintages in the planning forms.

If not, you must upgrade them, as well.

Installing New Firmware on the P330 Stack Processor

To install P330 stack processor firmware

1. From your S8300 telnet session, telnet back to the P330 stack processor:

Type `telnet <xxx.xxx.xxx.xxx>`

where `<xxx.xxx.xxx.xxx>` is the IP address of the P330 stack master processor on the customer's LAN.

2. At the **P330-1(configure)#** prompt, type

```
copy tftp SW_image <file> EW_archive <ew_file>
<tftp_server_address> <Module#>
```

where **<file>** is the full-path name for the image file with format and vintage number similar to viisa3_8_2.exe,

<ew_file> is the full-path name for the embedded web application file with format similar to p330Tweb.3.8.6.exe,

<tftp_server_ip_address> is the IP address of the TFTP server, and

<Module#> is the number, 1 through 10, of the media gateway in the stack. If there is only one G700 media gateway, the number is 1.

3. Verify that the download was successful when the prompt returns:

- type **show image version <module #>** and check the version number in the Version column for Bank B.
- type **dir <module #>** and check the version number in the ver num column for the EW_Archive file.

4. Type **reset <module #>**.

Installing new firmware on the G700 Media Gateway Processor

To install MGP firmware

- At the **P330-1(configure)#** prompt, type **session mgp** to reach the G700 media gateway processor.
- Type **configure** at the **MG-???-1(super)#** prompt to enter configuration mode, which will change the prompt to **MG-???-1(configure)#**.
- At the **MG-???-1(configure)#** prompt, type **show mgp bootimage** to determine which disk partition (bank) is in the **Active Now** column.

You will update the bank that is *not* listed as Active Now. The system displays the following screen:

Example: Show mgp bootimage

<u>FLASH MEMORY</u>	<u>IMAGE VERSION</u>
Bank A	109
Bank B	210
<u>ACTIVE NOW</u>	<u>ACTIVE AFTER REBOOT</u>
Bank B	Bank B

4. At the **MG-???-1(configure)#** prompt, type

```
copy tftp mgp-image <bank> <filename> <tftp_server_ip_address>
```

to transfer the mgp image from the tftp server to the G700,

where

<bank> is the bank that is *not* Active Now (Bank A in the example).

<filename> is the full path name of the mgp firmware image file, which begins with mgp and will be similar to the name mgp_8_0.bin.

<tftp_server_ip_address> is the IP address of the S8300.

For example:

```
copy tftp mgp-image a mgp_8_0.bin 195.123.49.54
```

The screen shows the progress.

5. Type **set mgp bootimage <bank>**

where **<bank>** is the same letter you entered in the previous step.

6. At the **MG-???-1(configure)#** prompt, type **reset mgp**.

A system prompt asks you to confirm the reset.

7. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

8. When the **P330-1(super)#** prompt appears, type **session mgp**.

9. At the **MGP-???-1(super)#** prompt, type **configure**.

10. Verify that the download was successful when the prompt returns.

Type **show mg list_config**.

The system displays the list of software.

Example: Show mg list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	230 (A)	67
V1	ICC	S8300	A	72	00	N/A
V2	DCP	MM712	A	2	58	N/A
V3	ANA	MM711	A	2	57	N/A
V4	DS1	MM710	A	1	58	N/A

Installing new firmware on the media modules

For upgrades of active media modules, you need to take the media modules out of service before initiating the upgrade process. To do this, go to a SAT session on the primary controller and issue a **busyout** command.

Note:

Skip this busyout procedure if the media modules are not in service; for example during an initial installation.

To busyout board (for active media modules)

1. Go to a SAT session on the primary controller and enter the command,
busyout board vx
where **x** is the slot number of the media module to be upgraded.
2. Verify the response,
Command Successfully Completed
3. Repeat for each media module to be upgraded.

To install media module firmware

1. Be sure that you have checked for the current vintage of the VoIP Module for the v0 slot (on the G700 motherboard).
This VoIP module does not occupy a physical position like other media modules.
2. At the **P330-1(configure)#** prompt, type **session mgp**.
3. At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.
4. Type **copy tftp mm-image v<slot #> <filename mm>**
<tftp_server_ip_address>
where
<slot #> is the slot of the specific media module,

<filename mm> the full-path name of the media module firmware file in a format such as mm712v58.fdl, and

<tftp_server_ip_address> is the ip address of the S8300.
Two or three minutes will be required for most upgrades. The VoIP media module upgrade takes approximately 5 minutes. Screen messages indicate when the transfer is complete.
5. After you have upgraded all the media modules, verify that the new versions are present.
At the **MG-???-1(configure)#** prompt, type **show mg list_config**
The list of software appears.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
V0	G700	DAF1	A	00	21.25.0 (A)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

- In the **TYPE** column, find the particular media module (v1 through v4), then check the matching field in the **FW VINTAGE** column to see if it matches the planning documentation.

Note:

Slot V1 can contain either a media module or the S8300, which will show as
TYPE ICC.

- Check the **VOIP FW** column and row for slot v0 to see if the number matches the VoIP firmware identified in the planning documentation.
- Type `reset <module #>`
where `<module #>` is the number of the G700 in the stack.
- When the reset is finished, type `show mm` to verify the upgrade.

To release board (if media module was busied out)

- When the upgrade procedure is complete, go to the SAT session and release the board
Type `release board vx`
where `x` is the slot number of the upgraded media module.
- Verify the response,
Command Successfully Completed

Note:

If you see the response, Board Not Inserted, this means that the media module is still rebooting. Wait one minute and repeat the `release board` command.

- Repeat the `release board` command for each media module that was busied out.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 stack processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* (available at <http://www.avaya.com/support>).

Administer Communication Manager



Important:

The administration procedures in this section are done on the media server that is the primary controller for the new G700 you previously installed. This primary controller may or may not be the S8300 you installed in the G700.

The primary controller for the G700/S8300 you are installing must be administered to enable communication between the primary controller and the G700/S8300. The administration differs somewhat depending on whether the primary controller is an S8300 or the primary controller is an S8400, S8500, or S8700-series Media Server.

When the primary controller is an S8300, it could be:

- The S8300 you previously installed
- A separate, possibly remote, S8300.

In the first case, the G700/S8300 you installed is a standalone (or “ICC”) configuration. In the second case, the S8300 you installed is configured as an LSP.

Perform one of the following two administration procedures in this section:

- [Administering an S8300 primary controller](#)
- [Administering an S8400, S8500, or S8700-series primary controller](#)

Administering an S8300 primary controller



CAUTION:

This administration applies only to the primary controller. If the S8300 you installed is configured as an LSP, do *not* perform this administration on it. Translations are automatically copied to the LSP from the S8300 primary controller.

Skip this section and go to [Administering an S8400, S8500, or S8700-series primary controller](#) on page 470 if the primary controller is an S8400, S8500, or S8700-series Media Server.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of administration required, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

In this section, you will use the SAT interface to:

- [Assigning Node Names and IP Addresses for the LSPs](#)
- [Administering Network Regions](#)
- [Associating LSPs with Network Regions](#)
- [Administering IP Interfaces](#)
- [Identifying LSPs to the S8300 primary controller](#)



CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Log in, and open a SAT session (type **sat** or **dsat**).
3. At the SAT prompt, type **reset system 4**
The system reboots.
4. After the reboot is complete, telnet to the S8300, login, and open a SAT session.

Assigning Node Names and IP Addresses for the LSPs

If the S8300 network configuration includes LSPs, they must be specified on the **Node Names** screen.

To assign node names

1. At the S8300 SAT prompt, type **change node-names ip** to open the **Node Names** screen.

Example Node Names Screen

change node-names ip		Page 1 of 1	
IP NODE NAMES			
Name	IP Address	Name	IP Address
default_____	0__ . 0__ . 0__ . 0__	_____	__ . __ . __ . __
node-10-lsp	192.168.1 . 50	_____	__ . __ . __ . __
node-11-lsp	192.168.1 . 51	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __

2. Enter the name and IP addresses for the LSPs.
3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 as primary controller, there will usually be one network region, defined as **1**. The procedure below uses 1 for the network region number as an example but the procedure applies for any network region number from 1 to 250.

To define IP network region 1



CAUTION:

Defining IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

1. At the SAT prompt, type **change ip-network-region 1**.

The S8300 displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:	Home Domain:	
Name:		
	Intra-region IP-IP Direct Audio:	yes
MEDIA PARAMETERS	Inter-region IP-IP Direct Audio:	yes
Codec Set: 1	IP Audio Hairpinning?	y
UDP Port Min: 2048		
UDP Port Max: 3028	RTCP Reporting Enabled?	n
	RTCP MONITOR SERVER PARAMETERS	
	Use Default Server Parameters?	y
DiffServ/TOS PARAMETERS		
Call Control PHB Value: 34		
Audio PHB Value: 46		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled?	n
H.323 Link Bounce Recovery?	y	
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. If necessary, complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. Press **F3 (Enter)** to submit the screen.

Associating LSPs with Network Regions

If the primary controller has LSPs, you can associate each LSP with one or more network regions. In the event of a network failure, IP telephones assigned to a network region will register with an LSP associated with that region.

This procedure associates up to six LSPs with a network region.

To associate LSPs with a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be associated with region 1.
The LSP names must be the same as administered on the **Node Names** screen.
3. Submit the form.
4. Repeat for each network region with which you want to associate LSPs.

Administering IP Interfaces

This procedure assigns network region 1, as an example, to the S8300 media server.

To assign the network region and IP endpoint access to the S8300

1. At the SAT prompt, type **change ip-interfaces procr.**

The S8300 displays the **IP Interfaces** screen for the media server.

IP Interfaces Screen

```

change ip-interfaces procr                                     Page 1 of 1

                                IP INTERFACES

                                Type: PROCR

                                Node Name: procr
                                IP Address: 135.9.41.146
                                Subnet Mask: 255.255.255.0

                                Enable Ethernet Port? y
                                Network Region: 1
                                Allow H.323 Endpoints? y
                                Allow H.248 Gateways? y
                                Gatekeeper Priority: 5

```

2. The field **Enable Ethernet Port?** should indicate **y** (yes). The **Node Name** should be the IP address of the S8300 media server.
3. In the **Allow H.323 Endpoints** field, enter a 'y' to allow H.323 endpoint connectivity to the server.
4. In the **Allow H.248 Endpoints** field, enter a 'y' to allow H.248 media gateway connectivity to the server.
5. In the **Gatekeeper Priority** field, enter a value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to **y**.

Identifying LSPs to the S8300 primary controller

If the primary controller has LSPs, you must enter the LSP node names on the Survivable Processor form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the **LSP** screen, their status can be viewed with the **list survivable-processor** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **Survivable Processor** screen.

1. At the SAT command line, type **add survivable-processor <name>**, where **<name>** is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 47: Add Local Survivable Processor screen

<pre>add survivable-processor sv-mg2-lsp</pre>	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET Node Name: sv-mg2-lsp IP Address: 128.256.173.101 Type: LSP Network Region: 1	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Skip to [Administering the Media Gateway](#) on page 480.

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

In this case, the S8300 you have installed is configured as an LSP.

 CAUTION:

This administration applies only to the primary controller that controls the S8300 LSP that you are installing. The primary controller can be an S8400, S8500, or S8700-series Media Server. Do *not* administer the S8300 LSP. Translations are automatically copied to the LSP from the primary controller.

Skip this section and go to [Administering an S8300 primary controller](#) on page 464 if the primary controller is an S8300.

Note:

Some of the procedures in this section may have been completed previously as part of a normal media server installation.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of required administration, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

In this section, you will use the SAT interface on the primary controller to:

- [Assigning Node Names and IP Addresses for the C-LANs and LSPs](#)
- [Administering Network Regions](#)
- [Assigning LSPs to the Network Regions](#)
- [Administering IP Interfaces](#)
- [Identifying the Survivable Processor on the primary controller](#)

Note:

For information on installing the CLAN boards on the S8400, S8500, or S8700-series port networks and complete information on installing an S8400, S8500, or S8700-series Media Server, see the Installation documentation on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

Assigning Node Names and IP Addresses for the C-LANs and LSPs

Note:

The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the media server. For information on how to upgrade the firmware on the S8400, S8500 or S8700-series Media Server, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Media Servers and Gateways*, 03-300412.

To assign node names and IP addresses

Note:

At the SAT prompt, type **change node-names ip** to open the **Node Names** screen.

Example Node Names Screen

change node-names ip		Page 1 of 1	
IP NODE NAMES			
Name	IP Address	Name	IP Address
default_____	0___.0___.0___.0__	_____	___.*___.*___.*___
node-1-clan_____	192.168.1___.124	_____	___.*___.*___.*___
node-2-clan_____	192.168.1___.97	_____	___.*___.*___.*___
node-10-lsp_____	192.168.1___.50	_____	___.*___.*___.*___
node-11-lsp_____	192.168.1___.51	_____	___.*___.*___.*___
_____	___.*___.*___.*___	_____	___.*___.*___.*___
_____	___.*___.*___.*___	_____	___.*___.*___.*___
_____	___.*___.*___.*___	_____	___.*___.*___.*___

1. Enter the name and IP address for the C-LANs and LSPs.
2. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 LSP and an S8500 or S8700-series Media Server as the primary controller, there may be more than one network region, since there can be up to 250 G700 media gateways connected to the S8500 or S8700-series Media Server with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700-series port networks, though they may also have the same network region.

Note:

With an S8300 or an S8400 Media Server, there still may be a need for more than one network region, though the S8400 supports up to five media gateways and the S8300 supports up to 50 media gateways.

The G700, in the case of multiple network regions, may also share the same network region as the CLAN board(s). However, it may have a different network region because of the geographic distances of the connections between the G700 and the primary controller. The G700 network region may also differ because of the nature of the endpoints connected to it.

To configure IP network regions for the G700 and CLAN board(s)



CAUTION:

Configuring IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

1. On the SAT screen of the primary controller for the G700 media gateway, type **change ip-network-region <network_region>**

where **<network_region>** is the region you will assign to the G700 media gateway. This region number may or may not match the network region of the S8400, S8500, or S8700-series CLAN boards.

The system displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain:	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 3048		
DiffServ/TOS PARAMETERS	RTCP Reporting Enabled? n	
Call Control PHB Value: 34	RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters? y	
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. Complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. If the network region of the G700 (1 in this example) is different from that of the S8400, S8500, or S8700-series CLAN board(s), you must interconnect the two regions.

Press **NextPage** twice to display page 3, of the **Inter Network Region Connection Management** screen.

This screen shows the source region (1) and the first 15 destination network region numbers. (Pages 4–19 show destination regions 16–250).

IP Network Region Screen, Page 3

display ip-network-region 1									
Inter Network Region Connection Management									
src	dst	codec	direct				Dynamic	CAC	
rgn	rgn	set	WAN	WAN-BW-limits	Intervening-regions		Gateway		IGAR
1	1	1							
1	2								
1	3								
1	4								
1	5								
1	6								
1	7								
1	8								
1	9	3							
1	10								
1	11								
1	12								
1	13								
1	14								
1	15								

4. Type the number for the type of codec set (1–7) that the S8400, S8500, or S8700-series Media Server will use to interconnect the G700 and the C-LAN board(s) in the row corresponding to the region of the C-LAN.

In this example, the C-LAN is in region 9 and codec-set type 3 is to be used for the interconnection between region 1 and region 9. (In this example, codec type 1 is used for communication within region 1)

The SAT command, **list ip-codec-set**, lists the types of codecs available on this server.

For more detail about the Inter Network Region Connection Management form, see *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

5. Press **F3 (Enter)** when complete.

Assigning LSPs to the Network Regions

If the primary controller has LSPs, you can assign the LSPs to network regions. In the event of a network failure, IP telephones assigned to a network region will register with the LSPs assigned to that region.

This procedure assigns up to six LSPs to a network region.

To assign LSPs to a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be assigned to region 1.
The LSP names must be the same as administered on the **Node Names** form.
3. Submit the form.
4. Repeat for each network region to which you want to assign LSPs.

Administering IP Interfaces

To define the IP interfaces of the S8400, S8500, or S8700-series port network CLAN boards

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type **change ip-interfaces <slot location>** to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces 01a03	Page 1 of 1
IP INTERFACES	
Type: C-LAN Slot: 01A03 Code/Suffix: TN799 d Node Name: procr IP Address: 135.9.41.146 Subnet Mask: 255.255.255.0 Gateway Address: 135.9.41.254 Enable Ethernet Port? y Network Region: 1 VLAN: 0 Link: 1 Allow H.323 Endpoints? y Allow H.248 Gateways? y Gatekeeper Priority: 5 Target socket load: Receive Buff TCP Window Size:	
ETHERNET OPTIONS	
Auto? n Speed: 100 Mbps Duplex: Full	

2. Complete the fields as described the in [Table 30](#).

Table 30: IP interfaces field descriptions

Field	Conditions/Comments
Type	Either C-LAN.
Slot	The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799 for C-LAN.
Node name	The unique node name for the IP interface. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the C-LAN.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see <i>“Administration for Network Connectivity for Avaya Communication Manager, 555-233-504”</i> .
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.

1 of 2

Table 30: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
VLAN	The VLAN number assigned to the C-LAN, if any.
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Receive Buffer TCP Window Size	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.
Link	This display only field shows the unique number for the Ethernet link. The Ethernet link was assigned on the data module form.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
Auto?	Enter 'y' or 'n' to set auto-negotiation.
Speed	Enter 10 or 100 Mbps if Auto was set to no.
Duplex	Enter half or full if Auto was set to no.

2 of 2

3. Close the screen.

To define the IP interface of the S8400 or S8500 processor Ethernet port**Note:**

This should have already been established as a part of normal S8400 or S8500, Media Server installation.

1. Type `change ip-interfaces procr` to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces procr		Page 1 of 1
IP INTERFACES		
Type: PROCR		
Node Name: procr		
IP Address: 135.9.41.146		
Subnet Mask: 255.255.255.0		Link: 1
Enable Ethernet Port? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
Target socket load:		

2. Complete the fields as described the in [Table 31](#).

Table 31: IP interfaces field descriptions

Field	Conditions/Comments
Type	Display only. PROCR
Node name	The unique node name for the IP interface. procr is the default node name. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the Processor Ethernet.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see <i>“Administration for Network Connectivity for Avaya Communication Manager, 555-233-504”</i> .
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.

1 of 2

Table 31: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
2 of 2	

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the LSP form, their status can be viewed with the **list survivable-processor** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

1. At the SAT command line, type **add survivable-processor <name>**, where **<name>** is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 48: Add Local Survivable Processor screen

<pre>add survivable-processor sv-mg2-lsp</pre>	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET Node Name: sv-mg2-lsp IP Address: 128.256.173.101 Type: LSP Network Region: 1	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Administering the Media Gateway

To perform the procedures in this section, SSH to the primary controller, log in, and open a SAT session.



CAUTION:

Before administering a media gateway, make sure that the gateway has been fully configured.

In this section, you will do the procedures:

- [To add a media gateway](#)
- [To verify changes](#)
- [To enable announcements, if necessary](#)
- [To save Communication Manager translations](#)

To add a media gateway

1. At the SAT prompt, type `add media-gateway <number>`

where `<number>` is the gateway number from 1 to *n*. (*n* is 50 for an S8300, 5 for an S8400, and 250 for an S8500 or S8700-series Media Server).

The **Media Gateway** screen appears.

Add media gateway Screen

add media-gateway 1		Page 1 of 1
MEDIA GATEWAY		
Number: 1	Registered:	
Type: g700	FW Version/HW Vintage:	
Name: Swainsons	IP Address:	
Serial No: 012X06230551	Controller IP Address:	
Encrypt Link? y	MAC Address: 00:04:0d:02:06:ca	
Network Region: 1	CF: 8 MB	
Location: 1	Site Data:	
Recovery Rule: none		
Slot	Module Type	Name
V1:		
V2:		
V3:		
V4:		
V9:		

2. Complete the **Name** field with the hostname assigned to the G700 media gateway.
3. Complete the **Identifier** field with the serial number of the G700 media gateway.

You can obtain the serial number by typing the **show system** command at the MGP command line interface.

**CAUTION:**

Be sure the serial number for the G700 media gateway you enter in this procedure matches *exactly* the serial number displayed in the **show system** command. The serial number is case-sensitive, and if entered incorrectly, will prevent the S8300 media server from communicating with the G700 media gateway.

4. Complete the **Network Region** field with the value supplied in the planning documentation.
5. If specifically requested by the customer or your planning documents, type **gateway-announcements** in the V9 field.

This field allows you to enable announcements on the G700 media gateway. V9 is a virtual slot. There is no announcement board associated with it. The announcements for the G700 are available in the G700 firmware and are administered in the same way as announcements on the TN2301 circuit pack used on S8400, S8500, or S8700-series port networks.

If there are multiple G700 media gateways sharing announcements, then enable announcements on the G700 whose trunks will receive the announcements most often.

6. Press **F3 (Enter)** to save your changes.

If properly administered, the G700 should register with the primary controller within 1–2 minutes. The **IP Address**, **MAC Address**, and **Module Type** fields are populated automatically after the G700 media gateway registers with the server.

7. Type **change media-gateway** to view the **Media Gateway** screen.

Media Gateway screen (after registration with primary controller)

```

change media-gateway 1                                     Page 1 of 1

                                MEDIA GATEWAY

      Number: 1                      Registered: y
      Type: g700                     FW Version/HW Vintage: 21.13.0 /0
      Name: Swainsons                IP Address: 135.9.41.150
      Serial No: 012X06230551        Controller IP Address: 135.9.41.146
      Encrypt Link? y                MAC Address:
      Network Region: 1              CF: 8 MB
      Location: 1                    Site Data:
      Recovery Rule: none

      Slot  Module Type      Name
      V1:   S8300            ICC MM
      V2:   MM712            DCP MM
      V3:   MM711            ANA MM
      V4:   MM710            T1/E1 MM

      V9:
  
```

The media modules installed in the G700 are listed next to their slot numbers. Verify that a G700 media gateway has been successfully added.

To verify changes

1. At the SAT prompt, type **list media-gateway**.

Media-Gateway Report screen

```

list media-gateway

                                MEDIA-GATEWAY REPORT
  
```

Num	Name	Serial No/ FW Ver/HW Vint	IP Address/ Cntrl IP Addr	Type	NetRgn RecRule	Reg?
1	LabA	01DR07128730 21 .13 .0 /0	135.177.49.57 135.177.49.59	g700	1 1	y
2	Data MG2	02DR01130356 11 .2 .0 /0	135.177.49.90 135.177.49.40	g350	1 none	n

2. Verify that the G700 media gateway has registered.

The `y` in the registered field signifies that the G700 media gateway has registered. If the G700 should become unregistered, the `y` will become an `n`, but the IP address will remain assigned to the G700 media gateway. If the G700 has never been registered, the IP Address field will be blank.

If the G700 fails to register, two common causes are:

- The serial number added as the **Identifier** for the G700 is wrong. To check, log back into the G700 gateway and type `show system`. Check the serial number that appears.
- There is no IP connection between the G700 and the S8300. To check, type `show mgc` and then `ping mgp <controller_address>`.

To enable announcements, if necessary

1. *Only if specifically requested by the customer or your planning documents*, at the SAT prompt, type `enable announcement-board <gateway_number> v9`

where `<gateway_number>` is the number of the G700 media gateway you added.

`v9` is the virtual slot (for example, `2v9` means media gateway number 2, slot V9).

2. Press **Enter** to enable announcements.

The system displays the message

```
Command successfully completed
```

To save Communication Manager translations

Save translations again after all Communication Manager administration is complete.

1. At the SAT prompt, type `save translation`

Considerations for IP Phones Supported by a Local Survivable Processor

A DHCP server assigns IP addresses to IP endpoints dynamically. Avaya IP phones perform a DHCP discover request to receive an IP address, as well as receive parameters necessary to function correctly. These parameters include the location of the call control server, the location of the TFTP server, as well as the directory on the TFTP server from which the phone receives its upgrades.

When preparing a DHCP server to work with Avaya IP phones, there is an option that must be administered to allow the Avaya phone to receive the DHCP offer. This option is “site-specific-option-number” (sson) 176. Different DHCP servers allow for this administration in different ways, but the sson option must be mapped to 176. Then the option can be set up to send the information desired to the Avaya phones for the intended activity.

The sson option sends a string that includes the IP address of the Avaya Call Controller with which the phone will register (“MCIPADD=www.xxx.yyy.zzz”). In an S8400, S8500, or S8700-series system, this can be a CLAN address; in an S8400 or S8500, this can also be the IP address for the server’s port that is enabled for processor ethernet; in an S8300 system, this is the IP address of the S8300. Multiple addresses can be administered to allow for LSP failover. The second address in the MCIPADD list may be an IP address for a second CLAN board or an LSP. If a second CLAN board is used, then the third address must be the LSP, and any subsequent addresses should be alternate LSPs. Local LSPs should appear first in the list, with remote LSPs later in the list as possible back ups.

If an IP phone loses its connection to the primary controller, it will try to register with an LSP associated with its network region (as defined on page 3 of the IP Network Region form). However, if the phone resets, it loses this information and goes to the DHCP server for a controller. If the only controller in the MCIPADD list is the primary controller, and if the connection to the primary controller is down, the phone cannot register. Having an LSP in the MCIPADD list gives the IP phones an alternate controller in this situation.

Note:

It is strongly recommended that at least one LSP be administered in the MCIPADD list.

Also included in the sson option string is the “MCPORT=1719”. This is the port the phone will listen on for signalling traffic to the call controller. Next is the tftp server field. This field indicates to the phone where it is to receive firmware service packs, along with the tftp directory field.

All phones for which the DHCP server has an LSP as the second address in the MCIPADD list should be administered to be in the same network region. Or, if administered to be in different network regions, the network regions involved should be interconnected. Use the `ip-network-map` form on the primary controller to put the IP phones in the same network region. On the `ip-network-map` form, a range of IP addresses (or a subnet) can be specified to be in a single network region. Enter the IP address range, or subnet, that contains the IP addresses of the IP phones and enter the desired network region number for that address range. The same address range or subnet must then be administered on the DHCP server. If it is not desired that all the phones be in the same network region, the form “`ip-network-region #`” should be used to interconnect all the network regions that contain those phones.

Transition of Control from Primary Controller to LSP

When the network connection between the G700 and the S8300, S8400, S8500, or S8700-series primary controller goes down, control of endpoints connected to the G700 goes to the next point in the primary controller list, which will be either a second CLAN board or the LSP. At this point, the primary controller alarms to notify the customer and services personnel that the network connection between the primary controller and G700 has problems. If control passes to the LSP, the LSP's license allows it to support the G700 endpoints for up to 30 days, within which the network problems should be resolved.

The customer may pass control back to the S8300, S8400, S8500, or S8700-series primary controller manually, by selecting **Shutdown this server** from the S8300 web page (includes selecting the option to restart after shutdown), or a technician must run `reset system 4` from the Linux command line. When the system reboots, the G700 and its endpoints reregister with the primary controller.

The customer may also choose to administer Communication Manager on the System Parameters Media Gateway Automatic Recovery Rule screen, such that the primary controller accepts control back from the LSP as soon as possible, based on whether there are calls active or what time of day it is. See *Administrator Guide for Avaya Communication Manager*, 03-300509.

Set Up SNMP Alarming on the G700

Setting up SNMP alarm reporting involves two main tasks:

- Configuring the primary server to report alarms to a services support agency
- Configuring the G700 Media Gateway to send its traps to a network management system (NMS)

Configuring the primary server to report alarms to a services support agency

The primary server may be an S8300, S8400, S8500, or S8700/S8710/S8720 Media Server. The media server supports two methods for reporting alarms. Either, both, or no alarm-reporting method may be used at a given site.

- **OSS Method.**

The server's software applications and hardware devices under its control can generate Operations Support System (OSS) alarms. These alarms are recorded in the server logs, and may be reported to Avaya's Initialization and Administration System (INADS), or another services support agency over the server's modem interface.

To provide OSS alarm notification, the server requires a USB connection to a modem that is connected to an analog line. The modem must be configured using the media server's Web Interface, in the **Set Modem Interface** screen, and enabled to send and receive calls using the **Enable/Disable Modem** screen.

Note:

Configuration of the OSS alarming method can only be done using Linux shell commands.

- **SNMP Method**

SNMP traps may be sent in User Datagram Protocol (UDP) to a corporate network management system (NMS) using the **Configure Trap Destinations** screen on the media server's Web Interface. The OSS and SNMP alarm-notification methods operate independently of each other; either or both may be used. Currently, the following NMSs are supported:

- Avaya Fault and Performance Manager, as a standalone application, or integrated within Avaya Network Management Console with VoIP SystemView
- Avaya Network Management Console with VoIP SystemView
- HP Openview

To provide SNMP alarm notification, on the server Web Interface use the **Configure Trap Destinations** screen to set up SNMP destinations in the corporate NMS.

Administering INADS phone numbers and Enabling alarms to INADS

The following procedure, using the primary server's Linux shell commands, administers the dial-out modem to send alarms in the OSS method. In this example, the primary server is an S8300, and the services support agency is Avaya's Initialization and Administration System (INADS).

Perform this task after all Communication Manager administration is complete.

Note:

Do these steps only if the S8300 is the primary controller and the customer has a maintenance contract with Avaya. Use the information you acquired from the ART tool (see [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 413).

Also, a USB modem must have already been installed.

To add INADS phone numbers and Enable alarms to INADS

1. With a direct connection to the S8300 Services port, open a telnet session and log in as *craft* (or *dadmin*).
2. At the Linux prompt, type `almcall -f INADS phone number -s <second-number>` and press **Enter**.
3. At the prompt, type `almenable -d b -s y` and press **Enter**.
4. Type `almenable` and press **Enter** to verify that the alarms are enabled.
5. Log off

Configuring the G700 Media Gateway to send its traps to a network management system (NMS)

Configuring the G700 Media Gateway to send SNMP traps to the primary server can be accomplished by two commands:

- P330 stack processor CLI command `set snmp community trap [community string]`
- Media Gateway Processor (MGP) CLI command `set snmp trap <IP address> enable`

Configuring an SNMP community string for traps

SNMP requires community strings to be used for each SNMP 'request'. You can set only three community strings on the G700 — one each for read requests, write requests, and traps.

To configure an SNMP community string for traps

1. Telnet to the P330 stack processor.
2. Log in as *root*.
3. At the **P330-1(super)#** prompt, type `set snmp community trap [community string]` and press **Enter**.
4. Type `exit`

Configuring the destination for G700 SNMP traps

Events occurring on the G700 cause SNMP traps to be generated. The G700 MGP can be configured to send SNMP traps to any network management system (NMS) in the network, including the primary server (S8300, S8400, S8500, or S8700-series Media Server). The MGP CLI `set snmp trap` command is the way to configure the NMS network element that will receive those traps.

The command syntax is:

```
set SNMP trap <IP address> {enable/disable}  
[{all|power|temp|app|module|config|voice|operations}]
```

where

`<IP address>` is the IP address of the NMS trap receiver that will be receiving the traps from the G700, and

`[{all|power|temp|app|module|config|voice|operations}]` indicates the groups whose traps will be sent to the specified receiver. If no keywords follow the IP address entry, then 'all' traps will be enabled for the specified receiver.

If 'enable' or 'disable' is used without a trap designation keyword, then 'all' traps is assumed. Up to ten trap receivers can be configured.

To configure the destination for G700 SNMP traps

1. At the **P330-1(super)#** prompt, type `session mgp`
2. At the **mg-xxx-n(super-user)#** prompt, type `configure` and press **Enter**.
3. At the **mg-xxx-n(configure)#** prompt, type
`set snmp trap <IP address> enable`
and press **Enter**.
4. Type `exit`

Complete the Installation of the S8300 (if the Primary Controller)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test the endpoints
- Administer Communication Manager for trunks, features, networking, or other items required by the customer
- Complete the electrical installation
- Enable adjunct systems

Note:

Follow the existing process and procedures to register the S8300.

Updating IA770 INTUITY AUDIX Messaging, if installed

Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update

After the upgrade is complete, perform the following post-upgrade tasks.

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing IA770 service pack (or RFU) files, if any

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at <http://support.avaya.com>.

1. Select **Messaging Administration** from the main menu.
2. Select **Utilities** from the Messaging Administration menu.
3. Select **Software Management** from the Utilities menu.
4. Select **Advanced Software Installation** from the Software Management menu.
5. Select **Continue this operation without current system backup**.
6. Select the IA770 update package and click **Install Selected Packages**.

Note:

The system automatically prompts you to restart INTUITY AUDIX when the service pack has been installed. Therefore, if you restart AUDIX at this time, you do *not* need to perform the following procedure, [Starting IA770 INTUITY AUDIX Messaging](#).

Starting IA770 INTUITY AUDIX Messaging

 CAUTION:

You do *not* need to perform this task if you restarted AUDIX as a part of the installation of the IA770 service pack.

After the IA770 INTUITY AUDIX Messaging application has been updated, you must restart it using the following steps:

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Start Messaging Software**.

The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Verifying start up of IA770 INTUITY AUDIX Messaging

To verify operation of IA770 INTUITY AUDIX Messaging, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.
the **View Process Status Results** screen displays.

View Process Status screen



View Process Status Results		
Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAlarmAgen	1/ 1	UP
C3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

[Help](#)

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an IA770 sanity test:
 - a. At the Linux command line, type `/vs/bin/display`
 - b. All states should be `Inserv` with an associated phone number.
 - c. Retrieve the test message saved before the upgrade.

If IA 770 fails to start after a new installation

If you have installed or upgraded IA 770 INTUITY AUDIX and it does not start, you must ensure that an IP address has been provided for use with IA 770. To check for the IP address, you must use the **Configure Server** option through the Maintenance Web pages.

On the Configure Interfaces screen, ensure that a valid IP address is present in the **Integrated Messaging** section.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **save translation** and press **Enter**.

When the save is finished, the system displays the message,

`Command successfully completed.`

Backing up the system

To back up the system to compact flash media (S8300C Media Server only)

1. Plug the cable to the compact flash drive into a USB port on the S8300C.
2. Insert a 128-Mb compact flash media into the top right slot of the drive.
3. On the S8300 main menu, select **Backup Now**.

The system displays the **Backup Now** screen.

4. Select the type of data you want to back up by selecting the appropriate data set.
5. Select Local Compact Flash Card back up the data onto the compact flash card.

Optionally, select Format Compact Flash to format a new card.

Note:

The compact flash card needs to be formatted only before the first use.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

To back up the system over the customer's LAN

1. Make sure you have the IP address of the customer's FTP, SFTP, or SCP backup server.
2. On the S8300 main menu, select **Backup Now**.

The system displays the **Backup Now** screen.

3. Select the type of data you want to back up by selecting the appropriate data set.
4. Select a backup method, normally **FTP**, **SFTP**, or **SCP**, to indicate the destination to which the system sends the backup data.
5. Complete the following fields:

- **User name**

You must enter a valid user name to enable the media server to log in to the FTP or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.

- **Password**

You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.

- **Host name**

Enter the DNS name or IP address of the FTP or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

- **Directory**

Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. The default directory for backup data on the FTP or SCP server is /var/home/ftp. If you do not want to use the default directory, you must enter the path name for the directory.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

This completes the installation of the G700 Media Gateway with an S8300 Media Server as primary controller.

If using IA770, administer Communication Manager for Integrated Messaging

A number of administration tasks must be performed to allow IA770 Integrated Messaging to work. These tasks are explained in detail in *Administering Media Servers to work with IA770*.



CAUTION:

IA770 INTUITY AUDIX Messaging processes messages using the G.711 codec only. Therefore, ensure that a codec set exists that uses only the G.711 codec. Then, assign that codec set to a network region. And, finally, assign that network region to the AUDIX signaling group that is linked to the IA770 INTUITY AUDIX Messaging trunk group.

If IA 770 fails to start after a new installation

If you have installed or upgraded IA 770 INTUITY AUDIX and it does not start, you must ensure that an IP address has been provided for use with IA 770. To check for the IP address, you must use the **Configure Server** option through the Maintenance Web pages.

On the Configure Interfaces screen, ensure that a valid IP address is present in the **Integrated Messaging** section.

Complete the Installation Process (for an S8300 LSP)

Consult the planning documentation to obtain the necessary information to complete the installation.

Part of the final process will be to:

- Connect and administer test endpoints
- Test endpoints
- Complete the electrical installation
- Enable adjunct systems

This completes the installation of the G700 Media Gateway with an S8300 LSP.

Chapter 9: Manual installation of a new G700 without an S8300

This chapter covers the manual procedures to install the firmware on an new Avaya G700 Media Gateway without an Avaya S8300 Media Server. The G700 is controlled by an external primary server running Avaya Communication Manager. The primary server can be an Avaya S8500 or S8700-series Media Server or an S8300 residing in another G700.

Note:

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

The following major tasks are covered in this chapter:

Before going to the customer site

- [Getting information that the project manager provides](#) on page 498
- [Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary](#) on page 498
- [Downloading G700 firmware files to your TFTP directory](#) on page 498

Configure the G700

- [Assigning the IP addresses of the G700 media gateway components](#) on page 501
- [Setting up the controller list for the G700](#) on page 506
- [Configuring an X330 Expansion Module \(If Necessary\)](#) on page 509

Prepare to install firmware on the G700

- [Accessing the P330 Stack Processor](#) on page 510
- [Verifying the contents of the tftpboot directory](#) on page 510

Install New Firmware on the G700 Media Gateway

- [Installing new firmware on the P330 stack processor](#) on page 513
- [Installing new firmware on the G700 Media Gateway Processor](#) on page 514
- [Installing new firmware on the media modules](#) on page 515
- [Setting rapid spanning tree on the network](#) on page 517

Administer an S8300 primary controller

- [Assigning Node Names and IP Addresses for the LSPs](#) on page 519
- [Administering Network Regions](#) on page 520
- [Associating LSPs with Network Regions](#) on page 521
- [Administering IP Interfaces](#) on page 522
- [Identifying the Survivable Processor on the primary controller](#) on page 523

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

- [Assigning Node Names and IP Addresses for the C-LANs and LSPs](#) on page 525
- [Administering Network Regions](#) on page 526
- [Assigning LSPs to the Network Regions](#) on page 528
- [Administering IP Interfaces](#) on page 529
- [Identifying the Survivable Processor on the primary controller](#) on page 533

Administer the Media Gateway

- [Administering the Media Gateway](#) on page 534
- [Complete the Installation Process](#) on page 538

Installation overview

What are the system components

About G700 components

A P330 Stack Processor is built into the G700 Media Gateway. (This processor is also known as the *Layer 2 switching processor*). In addition, the G700 contains:

- Media Gateway Processor (MGP)
- VoIP processor
- Up to four media modules
- Possibly an expansion module

Installing or upgrading the firmware for one or more of these processors and/or media modules is a required part of most new installations or upgrades.

About firmware files

You should obtain the firmware files for the G700 before going on-site. You can obtain the firmware files in bundled form on a CD or you can go to the Avaya Support website and download the individual firmware files onto your services laptop.

About the TFTP server

To install firmware on a G700 without an S8300 or LSP, you must first copy the firmware files to an external TFTP server on the customer LAN. The TFTP server can be a customer computer or it can be set up on your services laptop.

What provides initial access to the G700

Before the P330 stack processor is configured with an IP address, the only way to access it is with a direct connection from your laptop to the Console port on the G700. With this connection, you can assign the IP addresses to the G700 processors, which can then be accessed over the customer LAN.

Before going to the customer site

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

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary

A tar.gz file, which you obtain from a CD-ROM or a website, contains new G700 firmware. To load the firmware on a G700 Media Gateway, you must place this tar.gz file on a TFTP server that is connected to the customer's LAN. The TFTP server can be a customer computer or it can be your laptop if you have arranged with the customer to connect your laptop to the LAN.

Note:

A Linux or Unix TFTP server should be used only if the customer already has an existing one. In these cases, you download the tar.gz file to your laptop and give it to the customer for proper placement and execution.

To obtain the TFTP server software and install it, see [Appendix D: Install the Avaya TFTP server](#).

Downloading G700 firmware files to your TFTP directory

To install new firmware for the G700 processors and the media modules, you first need to move the new firmware files to a directory on the TFTP server. The installation program reads the new firmware files from this directory on the TFTP server.

Perform one of the two procedures in this section, depending on whether you have a bundled tar.gz file on a CD or wish to download individual firmware files from the Avaya Support website.

Downloading individual firmware files

Download the firmware files from the Web to your TFTP directory

Note:

The sequence of links on the website may be somewhat different than described here.

1. Access the <http://www.avaya.com/support> website.
2. Navigate to Firmware Downloads for The G700 Media Gateway.

The system displays a list of firmware files.

3. Locate the file names that match the files listed in your planning documentation.

The file names will approximate those listed in [Table 32: Firmware file formats](#):

Note:

The latest firmware versions may differ from those listed in [Table 32](#). Also, the appropriate firmware version may depend on the hardware vintage and/or on the release of Communication Manager. See *Communication Manager Software/ Firmware Compatibility Matrix* under Downloads on support.avaya.com.



CAUTION:

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Table 32: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_1_6.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.6.6.exe
G700 Media Gateway	mgp<version id>	mgp_24_21_1.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v57.fdl
8-port DCP Media Module	mm712<version id>	mm712v7.fdl
24-port analog Media Module	mm716<version id>	mm716v2.fdl
24-Port DCP Media Module	mm717<version id>	mm717v4.fdl
1 of 2		

Table 32: Firmware file formats (continued)

Component	Firmware Version Format	Example
8-port/trunk Analog Media Module (version 6 or earlier)	mm711<version id>	mm711v17.fdl
8-port/trunk Analog Media Module (version 7)	mm711<version id>	mm711h7v24.fdl
8-port/trunk Analog Media Module (version 20 or later)	mm711<version id>	mm711h20v68.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v67.fdl
T1/E1 Media Module	mm710<version id>	mm710v14.fdl
8-port BRI Media Module	mm720<version id>	mm720v6.fdl
2-port BRI Media Module	mm722<version id>	mm722v2.fdl
2 of 2		

4. Double-click the file name.
The system displays a **File Download** window.
5. Click on **Save this file to disk**.
6. Save the file to the **C:\tftp** directory (or your alternate tftp location).
7. Use WinZip or another zip file tool to unzip the file, if necessary.

Configure the G700

For a new installation of a G700 Media Gateway, you must complete the following configuration tasks:

1. [Assigning the IP addresses of the G700 media gateway components](#)
2. [Setting up the controller list for the G700](#)

Assigning the IP addresses of the G700 media gateway components

This section describes how to assign the IP addresses and IP routes to the G700 Media Gateway and its components. The IP addresses should be available to you on the IP Addressing Planning Form. The command arguments you will be supplying include:

- VLAN — Virtual Local Area Network: a defined network segment that allows users on that segment to have priority services in sharing information with each other.

If the network is not using VLANs, the VLAN should be 1. Otherwise, use the VLAN numbers indicated in your planning forms. The G700 Media Gateway should be assigned the same VLAN as the VLAN to which the Ethernet ports are connected. The P330 stack processor might or might not be assigned to the customer's network management VLAN.

- IP address — the unique identifier assigned to an entity on the customer LAN.
- Netmask — the subnet mask for the customer's LAN segment.
- Destination — distant networks to which the IP route command needs to send packets. Usually generalized to 0.0.0.0 for networks other than the local segment.
- default gateway — the gateway the ip route command specifies to get to the distant networks.

This section contains the following procedures:

- [To access the P330 stack processor](#)
- [To assign the IP address to the P330 stack processor](#)
- [To establish IP routing for the stack](#)
- [To check the serial number of the G700 media gateway processor](#)
- [To assign the IP address to the G700 media gateway processor](#)
- [To assign the default IP route to the G700 media gateway](#)
- [To assign IP addresses to the VoIP resources](#)
- [Checking for IP connections](#)

To access the P330 stack processor

1. Set up a direct connection to the G700 Console (serial) port and access the P330 stack processor using Hyperterminal (or similar terminal emulation application).
2. Login as *root*.

To assign the IP address to the P330 stack processor

1. At the **P330-1(super)#** prompt, type `nvrwam init` to initialize the default values of the media gateway processor.

This command ensures that any existing configuration information is cleared so you can enter the IP address and IP route information.

The system prompts you to verify that you want to erase the configuration.

2. Answer the prompt by typing `y(es)`.

The process re-initializes the G700 software back to factory defaults so new IP addresses can be stored correctly in the software. It also clears all configuration and administration on the G700 Media Gateway.

The G700 Media Gateway re-initializes.

3. Type `configure` to change to configuration mode.

4. At the **P330-1(configure)#** prompt, type `set interface inband <vlan> <ip_address> <netmask>` to assign an IP address to the P330 stack processor.

`<vlan>` is the vlan number, usually 1, to be established on the S8300 for the G700 Media Gateways. The `<ip_address> <netmask>` is the assigned address and subnet for the P330 stack processor.

5. Type `reset` and press **Enter** to reset the stack.

Select **Yes** at the dialog box that asks if you want to continue.

All LEDs flash. As the unit powers up, self-tests are run. When the G700 MPG or P330 stack processor has reset, login again to continue.

6. Login at the **Welcome to P330** menu.

The prompt **P330-1(super)#** appears.

7. Type `configure` to obtain the **P330-1(configure)#** prompt.

To establish IP routing for the stack

1. Type `show interface inband` to verify that the Avaya P330 stack server (Layer 2 Switching Processor) has the correct address.

2. Type `set ip route 0.0.0.0 <default-gateway>` to specify the gateway to handle addresses outside of the local subnet.

`<default-gateway>` is the IP address of the customer's default network gateway. This address should be available in the planning documentation.

3. Press **Enter** to save the destination and gateway IP addresses.

4. Type `show ip route`.

The route net and route host tables appear. Verify that the information is correct.

After you have configured the P330 stack processor, you assign an IP address to the G700 Media Gateway Processor (MGP). Your first task is to check the serial number of the MGP.

To check the serial number of the G700 media gateway processor

1. At the **P330-1(configure)#** prompt, type **session mgp**.
2. At the **MG-???-1(super)#** prompt, type **show system** to list various attributes of the G700.

The system displays a list of attributes, as shown in the following example:

Show System List for G700 Media Gateway

```

Welcome to Media Gateway Processor
FW version 25.25.0

MG-001-1<super># show system
Uptime(d,h:m:s): 8, 21:34:15
System Name      : -- Empty --
System Location  : -- Empty --
System Contact   : -- Empty --
MAC Address      : 00-04-0D-02-06-CA
Serial No        : 01DR12310260
Model No         : G700
HW Vintage       : 01
HW Suffix        : B
FW Vintage       : 25.25.0

Media Gateway Power Supplies
VOLTAGE(V)  ACTUAL(V)  STATUS
-----
DSP Complex  3.4        3.369    OK
MGP          5.1        5.099    OK
Media Modules -48.0     -48.360  OK
VoIP DSP     1.6        1.590    OK
VoIP 8260    2.5        2.480    OK

MG-001-1<super>#

```

3. Write the serial number on your planning document.

Make sure it matches the serial number sticker on the back of the G700 Media Gateway chassis. If there is a difference, the serial number in the displayed list is correct. You will need this later.

After you have assigned an IP address to the G700 processor, telnet directly to the G700 media gateway processor and login (the login name and password are provided in the planning documentation).

To assign the IP address to the G700 media gateway processor

1. At the **MG-???-n(super)#** prompt, type **configure** to change to configuration mode.
2. Type **nvram init** to initialize the default values of the media gateway processor.

This command ensures that any existing configuration information is cleared so you can enter the IP address and IP route information.

The system prompts you to verify that you want to erase the configuration.

3. Answer the prompt by typing **y(es)**.

This process re-initializes the G700 software back to factory defaults so new IP addresses can be stored correctly in the software. It also clears all configuration and administration on the G700 Media Gateway.

The G700 Media Gateway re-initializes.

4. At the **P330-1(configure)#** prompt, type **session mgp**.
5. At the **MG-???-1(super)#** prompt, type **configure** to change to configuration mode.
6. Type **set interface mgp <vlan> <ip_address> <netmask>** to assign an IP address to the G700 Media Gateway.

<vlan> is the vlan to be established on the customer's local network. This is usually **1**. The **<ip_address> <netmask>** is the assigned IP address and subnet for the G700 media gateway.



CAUTION:

If this G700 contains an S8300 configured as an LSP, use the VLAN administered on the primary controller.

7. At the **MG-???-n(configure)#** prompt, type **reset mgp**.

A system prompt asks to confirm the reset.

8. Select **Yes** at the dialog box that asks if you want to continue.

The G700 Media Gateway processor resets. The LEDs on the G700 Media Gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

9. At the **P330-1(configure)#** prompt, type **session mgp**.
10. At the **MG-???-1(super)#** prompt, type **configure** to reach the configuration level of the command line interface.
11. Type **show interface mgp** to verify that the G700 media gateway has the correct IP address.

To assign the default IP route to the G700 media gateway



CAUTION:

The default gateway IP routing address is *required* for Communication Manager 4.0.

1. At the **MG-???-n(configure)#** prompt, type

```
set ip route 0.0.0.0 0.0.0.0 <default_gateway>
```

to specify the gateway to handle addresses outside of the local subnet.

<default_gateway> is the IP address of the default network gateway. This address should be available in the planning documentation.

2. Type **show ip route mgp** to view the results.
3. Repeat Step 1 for additional ip routes, if needed.

Usually, only a default route is needed. Refer to your planning document.

From the G700 media gateway processor command line interface, you assign IP addresses to the VoIP resource resident on the G700 media gateway and to any installed MM760 VoIP media modules.

To assign IP addresses to the VoIP resources

1. At the **MG-???-n(configure)#** prompt, type **set interface voip <number> <ip address>**

<number> is the slot number of the VoIP media module. **v0** designates the VoIP resource resident on the G700 Media Gateway motherboard. The MM760 VoIP Media Modules are designated according the slot (for example, **v1**, **v2**, **v3**, **v4**) in which the media module has been installed.

<ip address> is the IP address of the VoIP resource.

For example: **set interface voip v0 132.236.73.3**

2. Type **show interface** to display a table of all configured interfaces, including all VoIP Media Modules.
3. Type **show voip v0** to display the VoIP resource on the motherboard.

Note:

It is not necessary to configure the VLAN, netmask, or IP routes for VoIP engines. The media gateway parameters are applied automatically.

Checking for IP connections

After you have assigned IP addresses to the P330 Stack Processor (Layer 2 Switching Processor), the G700 Media Gateway MGP, media modules, and the VoIP resources, validate the IP connections.

To run the ping command

1. At the **MG-???-n(config)#** prompt, type **ping mgp <IP_address>**

where **<IP_address>** is the address of an S8300, S8500, or S8700 Media Server, the VoIP engine, or any other functioning endpoint accessible on the customer's LAN. It is recommended to ping endpoints on both the same subnet and a different subnet.

Ping results appear on the screen, similar to the following example.

Ping MGP results

```
MG-???-1(configure)# ping mgp 135.122.49.55
PING 135.122.49.55: 56 data bytes
64 bytes from 135.122.49.55: icmp_seq=0. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=1. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=2. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=3. time=0. ms
64 bytes from 135.122.49.55: icmp_seq=4. time=0. ms
----135.122.49.55 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

2. Check that the same number of packets transmitted were also received.

3. Type **ping voip v0 <IP_address>**

<IP_address> is the address of the G700, or any other functioning endpoint on the customer's LAN.

Ping results appear on the screen, similar to the following example.

Ping VoIP results

```
MG-???-1(configure)# ping voip v0 135.122.49.55

----135.122.49.55 PING Statistics----
5 packets transmitted, 5 packets received, 0 packet loss
round-trip(ms) min/avg/max = 0/1/0
```

Setting up the controller list for the G700

To complete the configuration of the G700 media gateway, you need to administer a list of primary and alternate controllers. This list begins with the IP address of the primary controller. In the event that the G700 media gateway loses contact with its primary controller, it will seek to re-register with the primary controller first, then with the other controllers on this list. The other controllers are S8500 or S8700/S8710 media servers that can act as the primary controller, or S8300 media servers configured as Local Survivable Processors (LSPs).

Up to four IP addresses separated by commas can be entered to form the controller list.

To set the MGP controller list

1. At the **MG-???-n(configure)#** prompt, type the following commands to designate the primary, secondary, and LSP controllers for this G700:

- a. `clear mgc list`

- b. `set mgc list <ip_address> [, <ip_address> [, <ip_address> [, <ip_address>]]]`

where, the first `<ip_address>` can be one of the following IP addresses:

- For an S8700-series primary controller, the IP address of a C-LAN board that is connected to the primary controller.
- For an S8400 or S8500 primary controller, the IP address of either a C-LAN board that is connected to the primary controller, or an Ethernet port, on the server itself, that has been enabled for processor Ethernet connections.
- For an S8300 primary controller, the IP address of the S8300.

The next three `<ip_address>` parameters are optional IP addresses of up to three alternate controllers. Each of the three optional controllers can be a second C-LAN connected to the primary controller (S8400, S8500, or S8700-series Media Servers), an S8300 configured as an LSP, or the port enabled as the Ethernet processor port on an S8500 configured as an LSP. The types of alternate controllers in the list depend on the G700's primary controller and the other controller devices it supports.



CAUTION:

If you need to change the mgc list, you must run `clear mgc list` before running `set mgc list` again. You can also remove a single address in the list with the command `clear mgc list <ip address>`.

[Table 33](#) describes the possible optional controllers for an S8300 and S8700/S8710 primary controller:

Table 33: Possible optional controllers for various primary controllers

If primary controller is	Then, controller IP addresses can be
S8300	First: IP address of the S8300 primary controller. Next three: one, two, or three IP addresses of S8300s configured as LSPs.
S8400, S8500 or S8700, S8710, or S8720	First: IP address of the C-LAN for the S8400, S8500, or S8700/S8710/S8720 primary controller or IP address of processor Ethernet-enabled port on S8400 or S8500. Next three: one, two, or three IP addresses of alternate C-LANs and/or LSPs.

Note:

For an S8500 or S8700/S8710 primary controller, if you enter a combination of both C-LANs and LSPs, you must list C-LANs first.

2. Type **reset mgp** at the **MG-???-n(configure)#** prompt to reset the G700 media gateway processor.

A system prompt asks you to confirm the reset.

3. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

The system ultimately returns you to the **P330-1 (configure)** prompt.

At the **P330-1(configure)#** prompt, type **session mgp**.

At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.

Note:

Because the G700 media gateway has registered with its primary controller, the prompt name has changed; for example, to **MG-001-1**.

Type **show mgc** to display the list of available servers and their IP addresses.

For example:

Show Call Controller Status Screen

```
MG-001-1(configure)# show mgc
CALL CONTROLLER STATUS
-----
Registered           : YES
Active Controller    : 135.9.71.95
H248 Link Status     : UP
H248 Link Error Code: 0x0
MGC List Management  : Static

CONFIGURED MGC HOST          DHCP SPECIFIED MGC HOST
-----
135.9.71.95                  -- Not Available --
- Not Available --          -- Not Available --
- Not Available --          -- Not Available --
- Not Available --          -- Not Available --
```

The Gateway will have registered with the primary controller, if present. If the primary controller is running and has been administered properly, the **Registered** field says YES and the **H248 Link Status** says UP. If the controller is not running, the **Registered** field says NO and the **H248 Link Status** says DOWN.

Setting the LSP Transition Points

You must set the length of time that the G700 searches, in the event of a network problem, for primary controllers (for example, additional CLAN connections) with which to register. After this search time has elapsed, the G700 will search for an LSP with which to register. You must also set the total time the G700 searches for either a primary controller and an LSP, after which the G700 resets. And finally, you must define how many primary controllers, from 1 to 4, are in the controller list you just defined.

To set LSP transition points

1. At the **MG-001-1(configure)#** prompt, type `set mgp reset-times primary-search <search-time>`
where `<search-time>` is the time in minutes that the G700 searches for a primary controller before looking for an LSP. The range is from **1** to **60**.
2. At the **MG-001-1(configure)#** prompt, type `set mgp reset-times total-search <search-time>`
where `<search-time>` is the total time in minutes that the G700 searches for both primary controllers or LSPs. The range is from **1** to **60**.
3. At the **MG-001-1(configure)#** prompt, type `set mgp reset-times transition-point <#_of_primary>`
where `<#_of_primary>` is the number of primary controllers in the controller list. If the primary controller is an S8500 or S8700, the range is from **1** to **4**. If the primary controller is an S8300, `<#_of_primary>` must be **1**.

Configuring an X330 Expansion Module (If Necessary)

User Guides and Quick Start Guides for the expansion modules are available on the Avaya Support web site:

To configure an X330 Expansion Module

1. Go to the Avaya Support web site: <http://avaya.com/support>.
2. In the list on under Technical Database, click on **LAN, Backbone, and Edge Access Switches**.
3. Under Wiring Closet & Distribution, click on **P330 Stackable Switching System**.
4. Click on **All Documents**.
5. Select the appropriate document for the expansion module you are installing.

Prepare to install firmware on the G700

Before installing new firmware on the G700 processors and media modules, you must be:

- [Accessing the P330 Stack Processor](#)
- [Verifying the contents of the tftpboot directory](#)

Accessing the P330 Stack Processor

See [About connection and login methods](#) on page 41 for details on how to set up a connection and login.

Log on to the P330 stack processor using one of the following methods:

- Using a LAN connection, telnet to the IP address of the P330 stack processor and log in.
- If you are *not* using your laptop as the TFTP server, you can connect your laptop directly to the G700 Console (Serial) Port.

Then, use HyperTerm or a similar terminal emulation application to log in to the P330 stack processor Command Line Interface.

You are now logged-in at the Supervisor level with prompt **P330-1(super)#**.

Verifying the contents of the tftpboot directory

Before proceeding with the G700 firmware installation, you should check the */tftpboot* directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the */tftpboot* directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.
2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the */var/home/ftp/pub* directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the *pub* directory.

3. Copy the firmware files from the *pub* directory to the */tftpboot* directory, using the S8300 Media Server command line interface.

To copy firmware files to the */tftpboot* directory of an S8300 Media Server, do the following:

- a. Use SSH, Avaya Site Administration, or another tool to access the S8300 Media Server command line.

- b. Log in as craft.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to /var/home/ftp/pub.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the /tftpboot directory. To copy multiple firmware files (most firmware files have an .fdl suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the /tftpboot directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to /tftpboot.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

Conduct the following procedure to compare software versions running on the G700 processors and media modules with the versions in you planning documents. If the versions do not match, you need to install the new firmware for those components.

To determine if new firmware for the P330 stack processor is necessary

1. At either the **P330-1(super)#** or **P330-1(configure)#** prompt, type `dir`.

The system displays the directory list of software for the P330 stack processor.

Directory list for P300 stack processor

M#	file	ver num	file type	file location	file description
--	----	-----	-----	-----	-----
1	module-config Configuration	N/A	Running Conf	Ram	Module
1	stack-config	N/A	Running Conf	Ram	Stack Configuration
1	EW_Archive	4.0.4	SW Web Image	NV-Ram	WEB Download
1	Booter_Image	3.2.5	SW BootImage	NV-Ram	Booter Image

2. Check the version number (ver num) of the EW_Archive file to see if it matches the Release Letter.

If not, you must upgrade the P330 stack processor.

3. Type **show image version**

The system displays the list of software.

Show image version List for P330 stack processor

Mod	Module-Type	Bank	Version
-----	-----	----	-----
3	Avaya G700 media gateway	A	0.0.0
3	Avaya G700 media gateway	B	4.0.17

4. Check the version number of the stack software image file in Band B to see if it matches the your planning document.

If not, you must upgrade the P330 stack processor.

To determine if new firmware is required for the MGP, VoIP module, and installed media modules

1. Type **session mgp**

2. At the **MG-001-1(super)#** prompt, type **show mg list_config**

The system displays the list of software.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (B)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

3. Refer to the list to check the FW vintage number of the G700.

In the TYPE column, find G700, then check the matching field in the FW VINTAGE column to see if it matches the vintage number in your planning forms. If not, you must install new firmware on the G700 media gateway. Also check if the release number in the FW VINTAGE column contains (A) or (B) to designate the software bank. If the list shows B, you will upgrade A. If the list shows A, you will upgrade B.

4. Refer to the VOIP FW column and row for slot V0 (same row occupied by the G700 information) to see if the number matches the VoIP firmware identified in your planning forms.

If not, you must also upgrade the G700 media gateway motherboard VoIP module.

Note:

The VoIP processor on the motherboard is upgraded using the same firmware image file as the VoIP media modules; for example, the file mm760v8.fdl is vintage #8.

5. Check the FW VINTAGE column for vintages of each of the installed media modules: MM710, MM711, MM712, MM714, MM716, MM717, MM720, MM722, and/or MM760 to see if they match the FW vintages in the planning forms.

If not, you must upgrade them, as well.

Install new firmware on the G700 Media Gateway

The procedures in this section install firmware on the G700 processors and media modules.

Installing new firmware on the P330 stack processor

To install P330 stack processor firmware

1. See [Accessing the P330 Stack Processor](#).

2. At the **P330-1(configure)#** prompt, type

```
copy tftp SW_image <file> EW_archive <ew_file>
<tftp_server_address> <Module#>
```

where **<file>** is the full-path name for the image file with format and vintage number similar to viisa3_8_2.exe,

<ew_file> is the full-path name for the embedded web application file with format similar to p330Tweb.3.8.6.exe,

<tftp_server_ip_address> is the IP address of the TFTP server, and

<Module#> is the number, 1 through 10, of the media gateway in the stack. If there is only one G700 media gateway, the number is 1.

3. Verify that the download was successful when the prompt returns:
 - a. type **show image version <module #>** and check the version number in the Version column for Bank B.
 - b. type **dir <module #>** and check the version number in the ver num column for the EW_Archive file.
4. Type **reset <module #>**.

Installing new firmware on the G700 Media Gateway Processor

To install MGP firmware

1. At the **P330-1(configure)#** prompt, type `session mgp` to reach the G700 media gateway processor.
2. Type `configure` at the **MG-???-1(super)#** prompt to enter configuration mode, which will change the prompt to **MG-???-1(configure)#**.
3. At the **MG-???-1(configure)#** prompt, type `show mgp bootimage` to determine which disk partition (bank) is in the **Active Now** column.

You will update the bank that is *not* listed as Active Now. The system displays the following screen:

Example: Show mgp bootimage

<u>FLASH MEMORY</u>	<u>IMAGE VERSION</u>
Bank A	109
Bank B	210
<u>ACTIVE NOW</u>	<u>ACTIVE AFTER REBOOT</u>
Bank B	Bank B

4. At the **MG-???-1(configure)#** prompt, type

```
copy tftp mgp-image <bank> <filename> <tftp_server_ip_address>
```

to transfer the mgp image from the tftp server to the G700,

where

<bank> is the bank that is *not* Active Now (Bank A in the example).

<filename> is the full path name of the mgp firmware image file, which begins with mgp and will be similar to the name mgp_8_0.bin.

<tftp_server_ip_address> is the IP address of the S8300.

For example:

```
copy tftp mgp-image a mgp_8_0.bin 195.123.49.54
```

The screen shows the progress.

5. Type `set mgp bootimage <bank>`
where **<bank>** is the same letter you entered in the previous step.
6. At the **MG-???-1(configure)#** prompt, type `reset mgp`.
A system prompt asks you to confirm the reset.

7. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

8. When the **P330-1(super)#** prompt appears, type **session mgp**.

9. At the **MGP-???-1(super)#** prompt, type **configure**.

10. Verify that the download was successful when the prompt returns.

Type **show mg list_config**.

The system displays the list of software.

Example: Show mg list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	230 (A)	67
V1	ICC	S8300	A	72	00	N/A
V2	DCP	MM712	A	2	58	N/A
V3	ANA	MM711	A	2	57	N/A
V4	DS1	MM710	A	1	58	N/A

Installing new firmware on the media modules

For upgrades of active media modules, you need to take the media modules out of service before initiating the upgrade process. To do this, go to a SAT session on the primary controller and issue a **busyout** command.

Note:

Skip this busyout procedure if the media modules are not in service; for example during an initial installation.

To busyout board (for active media modules)

1. Go to a SAT session on the primary controller and enter the command,

busyout board vx

where **x** is the slot number of the media module to be upgraded.

2. Verify the response,

Command Successfully Completed

3. Repeat for each media module to be upgraded.

To install media module firmware

1. Be sure that you have checked for the current vintage of the VoIP Module for the v0 slot (on the G700 motherboard).

This VoIP module does not occupy a physical position like other media modules.

2. At the **P330-1(configure)#** prompt, type **session mgp**.
3. At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.
4. Type **copy tftp mm-image v<slot #> <filename mm>**
<tftp_server_ip_address>

where

<slot #> is the slot of the specific media module,

<filename mm> the full-path name of the media module firmware file in a format such as mm712v58.fdl, and

<tftp_server_ip_address> is the ip address of the S8300.

Two or three minutes will be required for most upgrades. The VoIP media module upgrade takes approximately 5 minutes. Screen messages indicate when the transfer is complete.

5. After you have upgraded all the media modules, verify that the new versions are present.

At the **MG-???-1(configure)#** prompt, type **show mg list_config**

The list of software appears.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (A)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

6. In the **TYPE** column, find the particular media module (v1 through v4), then check the matching field in the **FW VINTAGE** column to see if it matches the planning documentation.

Note:

Slot V1 can contain either a media module or the S8300, which will show as
 TYPE ICC.

7. Check the **VOIP FW** column and row for slot v0 to see if the number matches the VoIP firmware identified in the planning documentation.

8. Type `reset <module #>`
where `<module #>` is the number of the G700 in the stack.
9. When the reset is finished, type `show mm` to verify the upgrade.

To release board (if media module was busied out)

1. When the upgrade procedure is complete, go to the SAT session and release the board

Type `release board vx`

where `x` is the slot number of the upgraded media module.

2. Verify the response,

Command Successfully Completed

Note:

If you see the response, Board Not Inserted, this means that the media module is still rebooting. Wait one minute and repeat the `release board` command.

3. Repeat the `release board` command for each media module that was busied out.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 stack processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* (available at <http://www.avaya.com/support>).

Administer Communication Manager

Important:

The administration procedures in this section are done on the media server that is the primary controller for the new G700 you previously installed.

The primary controller for the G700 you are installing must be administered to enable communication between the primary controller and the G700. The administration differs somewhat depending on whether the primary controller is an S8300 or the primary controller is an S8400, S8500, or S8700-series Media Server.

Perform one of the following two administration procedures in this section:

- [Administering an S8300 primary controller](#)
- [Administering an S8400, S8500, or S8700-series primary controller](#)

Administering an S8300 primary controller

 CAUTION:

This administration applies only to the primary controller. If the S8300 you installed is configured as an LSP, do *not* perform this administration on it. Translations are automatically copied to the LSP from the S8300 primary controller.

Skip this section and go to [Administering an S8400, S8500, or S8700-series primary controller](#) on page 524 if the primary controller is an S8400, S8500, or S8700-series Media Server.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of administration required, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

 CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Log in, and open a SAT session (type **sat** or **dsat**).
3. At the SAT prompt, type **reset system 4**
The system reboots.
4. After the reboot is complete, telnet to the S8300, login, and open a SAT session.

Assigning Node Names and IP Addresses for the LSPs

If the S8300 network configuration includes LSPs, they must be specified on the **Node Names** screen.

To assign node names

1. At the S8300 SAT prompt, type **change node-names ip** to open the **Node Names** screen.

Example Node Names Screen

change node-names ip

Page 1 of 1

IP NODE NAMES

Name	IP Address	Name	IP Address
default	0.0.0.0		
node-10-lsp	192.168.1.50		
node-11-lsp	192.168.1.51		

- 2. Enter the name and IP addresses for the LSPs.
- 3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 as primary controller, there will usually be one network region, defined as **1**. The procedure below uses 1 for the network region number as an example but the procedure applies for any network region number from 1 to 250.

To define the network region for the S8300

**CAUTION:**
Defining IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see “*Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.”

- 1. At the SAT prompt, type **change ip-network-region 1**.
The S8300 displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain:	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 3048		
DiffServ/TOS PARAMETERS	RTCP Reporting Enabled? n	
Call Control PHB Value: 34	RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters? y	
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. If necessary, complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. Press **F3 (Enter)** to submit the screen.

Associating LSPs with Network Regions

If the primary controller has LSPs, you can associate each LSP with one or more network regions. In the event of a network failure, IP telephones assigned to a network region will register with an LSP associated with that region.

This procedure associates up to six LSPs with a network region.

To associate LSPs with a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be associated with region 1.
The LSP names must be the same as administered on the **Node Names** screen.
3. Submit the form.
4. Repeat for each network region with which you want to associate LSPs.

Administering IP Interfaces

This procedure assigns network region 1, as an example, to the S8300 media server.

To assign the network region to the S8300

1. At the SAT prompt, type **change ip-interfaces procr.**
The S8300 displays the **IP Interfaces** screen for the media server.

IP Interfaces Screen

```

change ip-interfaces procr                                     Page 1 of 1

                                IP INTERFACES

                                Type: PROCR

                                Node Name: procr
                                IP Address: 135.9.41.146
                                Subnet Mask: 255.255.255.0

                                Enable Ethernet Port? y
                                Network Region: 1

                                Allow H.323 Endpoints? y
                                Allow H.248 Gateways? y
                                Gatekeeper Priority: 5
  
```

2. The field **Enable Ethernet Port?** should indicate **y** (yes). The **Node Name** should be the IP address of the S8300 media server.
3. In the **Allow H.323 Endpoints** field, enter a 'y' to allow H.323 endpoint connectivity to the server.
4. In the **Allow H.248 Endpoints** field, enter a 'y' to allow H.248 media gateway connectivity to the server.
5. In the **Gatekeeper Priority** field, enter a value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **allow H.323 endpoints** field is set to **y**.

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the LSP form, their status can be viewed with the **list survivable-processor** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

1. At the SAT command line, type **add survivable-processor <name>**, where **<name>** is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 49: Add Local Survivable Processor screen

<pre>add survivable-processor sv-mg2-lsp</pre>	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET Node Name: sv-mg2-lsp IP Address: 128.256.173.101 Type: LSP Network Region: 1	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Skip to [Administering the Media Gateway](#) on page 534 to continue.

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

Complete the procedures in this section if the primary controller for the G700 you are installing is an S8400, S8500, or S8700-series Media Server. If the primary controller is an S8300, you should have completed the procedures in [Administering an S8300 primary controller](#) on page 519.

This document covers only the administration of Communication Manager required for the G700 media gateway to communicate with the primary controller over a customer's network. For the majority of required administration, see *Administrator Guide to Avaya Communication Manager*, 03-300509, or *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

For information on installing the CLAN boards on the S8400, S8500, or S8700-series Media Server port networks and complete information on installing an S8400, S8500, or S8700-series Media Server, see the Installation documentation on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

Assigning Node Names and IP Addresses for the C-LANs and LSPs

Note:

The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the S8400, S8500, or S8700-series Media Server. For information on how to upgrade the firmware on the C-LAN circuit pack, please see the "Upgrading firmware on programmable TN circuit packs," in *Upgrading, Migrating, and Converting Avaya Media Servers and Gateways*, 03-300412.

To assign node names and IP addresses

1. At the SAT prompt, type **change node-names ip** to open the **Node Names** screen.

Example Node Names Screen

change node-names ip		Page 1 of 1	
IP NODE NAMES			
Name	IP Address	Name	IP Address
default_____	0__ . 0__ . 0__ . 0__	_____	__ . __ . __ . __
node-1-clan_____	192.168.1 . 124	_____	__ . __ . __ . __
node-2-clan_____	192.168.1 . 97	_____	__ . __ . __ . __
node-10-lsp_____	192.168.1 . 50	_____	__ . __ . __ . __
node-11-lsp_____	192.168.1 . 51	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __
_____	__ . __ . __ . __	_____	__ . __ . __ . __

2. Enter the name and IP address for the C-LANs and LSPs.
3. Press **F3 (Enter)** when complete.

Administering Network Regions

Before assigning an IP network region to a G700, you must define network region on the IP Network Region form. After a network region is defined, you can assign it to the various network elements (servers, gateways, IP phones).

The information you need to do this should be provided in your planning documentation. Use the system defaults if the planning documentation does not specify otherwise.

For a G700 with an S8300 LSP and an S8500 or S8700-series Media Server as the primary controller, there may be more than one network region, since there can be up to 250 G700 media gateways connected to the S8500 or S8700-series Media Server with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700-series port networks, though they may also have the same network region.

Note:

With an S8300 or an S8400 Media Server, there still may be a need for more than one network region, though the S8400 supports up to five media gateways and the S8300 supports up to 50 media gateways.

The G700, in the case of multiple network regions, may also share the same network region as the CLAN board(s). However, it may have a different network region because of the geographic distances of the connections between the G700 and the primary controller. The G700 network region may also differ because of the nature of the endpoints connected to it.

To configure IP network regions for the G700 and CLAN board(s)



CAUTION:

Configuring IP network regions can be quite complex. For detailed information on the use and administration of IP network regions, see “*Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.”

1. On the SAT screen of the primary controller for the G700 media gateway, type **change ip-network-region <network_region>**

where **<network_region>** is the region you will assign to the G700 media gateway. This region number may or may not match the network region of the S8400, S8500, or S8700-series CLAN boards.

The system displays the **IP Network Region** screen.

IP Network Region Screen

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain:	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 3048		
DiffServ/TOS PARAMETERS	RTCP Reporting Enabled? n	
Call Control PHB Value: 34	RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters? y	
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 7		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

2. Complete the fields as described in *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Note:

It is strongly recommended to use the defaults in the screen. However, for the **RTCP Enabled** and **RSVP Enabled** fields, the entry should be **n** (no).

3. If the network region of the G700 (1 in this example) is different from that of the S8400, S8500, or S8700-series CLAN board(s), you must interconnect the two regions.

Press **NextPage** twice to display page 3, of the **Inter Network Region Connection Management** screen.

This screen shows the source region (1) and the first 15 destination network region numbers. (Pages 4–19 show destination regions 16–250).

IP Network Region Screen, Page 3

display ip-network-region 1									
Inter Network Region Connection Management									
src	dst	codec	direct				Dynamic	CAC	
rgn	rgn	set	WAN	WAN-BW-limits	Intervening-regions		Gateway		IGAR
1	1	1							
1	2								
1	3								
1	4								
1	5								
1	6								
1	7								
1	8								
1	9	3							
1	10								
1	11								
1	12								
1	13								
1	14								
1	15								

4. Type the number for the type of codec set (1–7) that the S8400, S8500, or S8700-series Media Server will use to interconnect the G700 and the C-LAN board(s) in the row corresponding to the region of the C-LAN.

In this example, the C-LAN is in region 9 and codec-set type 3 is to be used for the interconnection between region 1 and region 9. (In this example, codec type 1 is used for communication within region 1)

The SAT command, **list ip-codec-set**, lists the types of codecs available on this server.

For more detail about the Inter Network Region Connection Management form, see *“Administration for Network Connectivity for Avaya Communication Manager, 555-233-504.”*

5. Press **F3 (Enter)** when complete.

Assigning LSPs to the Network Regions

If the primary controller has LSPs, you can assign the LSPs to network regions. In the event of a network failure, IP telephones assigned to a network region will register with the LSPs assigned to that region.

This procedure assigns up to six LSPs to a network region.

To assign LSPs to a network region

1. On the **IP Network Region** screen, go to page 2.

IP Network Region Screen, page 2

change ip-network-region 1		Page 2 of 19
IP NETWORK REGION		
INTER-GATEWAY ALTERNATE ROUTING		
Incomming LDN Extension:		
Conversion to Full Public Number - Delete: Insert:		
Maximum Number of Trunks to Use:		
LSP NAMES IN PRIORITY ORDER		SECURITY PROCEDURES
1	node-10-LSP_____	1 challenge
2	_____	2
3	_____	3
4	_____	4
5	_____	5
6	_____	6

2. Enter the names of up to six LSPs to be assigned to region 1.
The LSP names must be the same as administered on the **Node Names** form.
3. Submit the form.
4. Repeat for each network region to which you want to assign LSPs.

Administering IP Interfaces

To define the IP interfaces of the S8400, S8500, or S8700-series port network CLAN boards

Note:

This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type **change ip-interfaces <slot location>** to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces 01A03	Page 1 of 1
IP INTERFACES	
Type: C-LAN Slot: 01A03 Code/Suffix: TN799 d Node Name: procr IP Address: 135.9.41.146 Subnet Mask: 255.255.255.0 Gateway Address: 135.9.41.254 Enable Ethernet Port? y Network Region: 1 VLAN: 0 Link: 1 Allow H.323 Endpoints? y Allow H.248 Gateways? y Gatekeeper Priority: 5 Target socket load: Receive Buff TCP Window Size:	
ETHERNET OPTIONS	
Auto? n Speed: 100 Mbps Duplex: Full	

2. Complete the fields as described the in [Table 34](#).

Table 34: IP interfaces field descriptions

Field	Conditions/Comments
Type	Either C-LAN.
Slot	The slot location for the circuit pack.
Code/Suffix	Display only. This field is automatically populated with TN799 for C-LAN.
Node name	The unique node name for the IP interface. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the C-LAN.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see <i>“Administration for Network Connectivity for Avaya Communication Manager, 555-233-504”</i> .
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.

1 of 2

Table 34: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.
VLAN	The VLAN number assigned to the C-LAN, if any.
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Receive Buffer TCP Window Size	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.
Link	This display only field shows the unique number for the Ethernet link. The Ethernet link was assigned on the data module form.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
Auto?	Enter 'y' or 'n' to set auto-negotiation.
Speed	Enter 10 or 100 Mbps if Auto was set to no.
Duplex	Enter half or full if Auto was set to no.

2 of 2

3. Close the screen.

To define the IP interface of the S8400 or S8500 processor Ethernet port**Note:**

This should have already been established as a part of normal S8400, S8500, or S8700-series Media Server installation.

1. Type `change ip-interfaces procr` to open the **IP Interfaces** screen.

IP Interfaces Screen

change ip-interfaces procr		Page 1 of 1
IP INTERFACES		
Type: PROCR		
Node Name: procr		
IP Address: 135.9.41.146		Link: 1
Subnet Mask: 255.255.255.0		
Enable Ethernet Port? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
Target socket load:		

2. Complete the fields as described the in [Table 35](#).

Table 35: IP interfaces field descriptions

Field	Conditions/Comments
Type	Display only. PROCR
Node name	The unique node name for the IP interface. The node name here must already be administered on the Node Names screen.
IP Address	The IP address (on the customer LAN) of the Processor Ethernet.
Subnet Mask	The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnetting, see <i>Administration for Network Connectivity for Avaya Communication Manager</i> , 555-233-504.
Enable Ethernet Port?	The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to its attributes on this screen.
Network Region	The region number for this IP interface.

1 of 2

Table 35: IP interfaces field descriptions (continued)

Field	Conditions/Comments
Target socket load	The threshold for the number of sockets used by this C-LAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated.
Allow H.323 Endpoints	Enter a 'y' to allow H.323 endpoint connectivity on this CLAN. Enter 'n' if you do not want H.323 endpoints to connect to this CLAN.
Allow H.248 Gateways?	Enter 'y' to allow H.248 gateway connectivity to this CLAN. Enter 'n' if you do not want H.248 gateways to connect to this CLAN.
Gatekeeper Priority	This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the allow H.323 endpoints field is set to a yes on this form.
2 of 2	

Identifying the Survivable Processor on the primary controller

If the primary server has LSPs, you must enter the LSP node names on the LSP form to enable the LSPs to get translations updates from the primary controller. Once the LSPs are successfully entered on the LSP form, their status can be viewed with the **list survivable-processor** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

1. At the SAT command line, type **add survivable-processor <name>**, where **<name>** is the LSP name from the Node Names screen.

The Survivable Processor screen appears.

Figure 50: Add Local Survivable Processor screen

<pre>add survivable-processor sv-mg2-lsp</pre>	Page 1 of xx
SURVIVABLE PROCESSOR - PROCESSOR ETHERNET Node Name: sv-mg2-lsp IP Address: 128.256.173.101 Type: LSP Network Region: 1	

2. The type field is automatically populated with **LSP**. **LSP** appears in the field if the node name is *not* associated with ESS.
3. Enter a network region for the LSP. The default is **1**. However, there may be a different network region better suited for the LSP to provide media gateway and IP phone support.

Skip to [Administering the Media Gateway](#) on page 534 to continue.

Administering the Media Gateway

To perform the procedures in this section, telnet to the primary controller, log in, and open a SAT session.



CAUTION:

Before administering a media gateway, make sure that the gateway has been fully configured.

In this section, you will do the procedures:

- [To add a media gateway](#)
- [To verify changes](#)
- [To enable announcements, if necessary](#)
- [To save Communication Manager translations](#)

To add a media gateway

1. At the SAT prompt, type `add media-gateway <number>`

where `<number>` is the gateway number from 1 to *n*. (*n* is 50 for an S8300, 5 for an S8400, and 250 for an S8500 or S8700-series Media Server).

The **Media Gateway** screen appears.

Add media gateway Screen

```

add media-gateway 1                                     Page 1 of 1

                                MEDIA GATEWAY

      Number: 1                      Registered:
      Type: g700                     FW Version/HW Vintage:
      Name: Swainsons                IP Address:
      Serial No: 012X06230551        Controller IP Address:
Encrypt Link? y                      MAC Address: 00:04:0d:02:06:ca
Network Region: 1                     CF: 8 MB
      Location: 1                     Site Data:
Recovery Rule: none

Slot  Module Type      Name
V1:
V2:
V3:
V4:

V9:

```

2. Complete the **Name** field with the hostname assigned to the G700 media gateway.
3. Complete the **Identifier** field with the serial number of the G700 media gateway.

You can obtain the serial number by typing the **show system** command at the MGP command line interface.

**CAUTION:**

Be sure the serial number for the G700 media gateway you enter in this procedure matches *exactly* the serial number displayed in the **show system** command. The serial number is case-sensitive, and if entered incorrectly, will prevent the S8300 media server from communicating with the G700 media gateway.

4. Complete the **Network Region** field with the value supplied in the planning documentation.
5. If specifically requested by the customer or your planning documents, type **gateway-announcements** in the V9 field.

This field allows you to enable announcements on the G700 media gateway. V9 is a virtual slot. There is no announcement board associated with it. The announcements for the G700 are available in the G700 firmware and are administered in the same way as announcements on the TN2301 circuit pack used on S8400, S8500, or S8700-series port networks.

If there are multiple G700 media gateways sharing announcements, then enable announcements on the G700 whose trunks will receive the announcements most often.

6. Press **F3 (Enter)** to save your changes.

If properly administered, the G700 should register with the primary controller within 1–2 minutes. The **IP Address**, **MAC Address**, and **Module Type** fields are populated automatically after the G700 media gateway registers with the server.

7. Type **change media-gateway** to view the **Media Gateway** screen.

Media Gateway screen (after registration with primary controller)

```

change media-gateway 1                                     Page 1 of 1

                                MEDIA GATEWAY

Number: 1                                           Registered: y
Type: g700                                           FW Version/HW Vintage: 21.13.0 /0
Name: Swainsons                                     IP Address: 135.9.41.150
Serial No: 012X06230551                             Controller IP Address: 135.9.41.146
Encrypt Link? y                                     MAC Address:
Network Region: 1                                     CF: 8 MB
Location: 1                                           Site Data:
Recovery Rule: none

Slot  Module Type      Name
V1:   S8300            ICC MM
V2:   MM712            DCP MM
V3:   MM711            ANA MM
V4:   MM710            T1/E1 MM

V9:

```

The media modules installed in the G700 are listed next to their slot numbers. Verify that a G700 media gateway has been successfully added.

To verify changes

1. At the SAT prompt, type **list media-gateway**.

Media-Gateway Report screen

```

list media-gateway

                                MEDIA-GATEWAY REPORT

```

Number	Name	Serial No/ FW Ver/HW Vint	IP Address/ Cntrl IP Addr	Type	NetRgn RecRule	Reg?
1	LabA	01DR07128730 21 .13 .0 /0	135.177.49.57 135.177.49.59	g700	1 1	y
2	Data MG2	02DR01130356 11 .2 .0 /0	135.177.49.90 135.177.49.40	g350	1 none	n

2. Verify that the G700 media gateway has registered.

The `y` in the registered field signifies that the G700 media gateway has registered. If the G700 should become unregistered, the `y` will become an `n`, but the IP address will remain assigned to the G700 media gateway. If the G700 has never been registered, the IP Address field will be blank.

If the G700 fails to register, two common causes are:

- The serial number added as the **Identifier** for the G700 is wrong. To check, log back into the G700 gateway and type `show system`. Check the serial number that appears.
- There is no IP connection between the G700 and the S8300. To check, type `show mgc` and then `ping mgp <controller_address>`.

To enable announcements, if necessary

1. *Only if specifically requested by the customer or your planning documents*, at the SAT prompt, type `enable announcement-board <gateway_number> v9`

where `<gateway_number>` is the number of the G700 media gateway you added.

`v9` is the virtual slot (for example, `2v9` means media gateway number 2, slot V9).

2. Press **Enter** to enable announcements.

The system displays the message

Command successfully completed

To save Communication Manager translations

Save translations again after all Communication Manager administration is complete.

1. At the SAT prompt, type `save translation`

Complete the Installation Process

Consult the planning documentation to obtain the necessary information to complete the installation. Part of the final process will be to:

- Connect and administer test endpoints
- Test the endpoints
- Complete the electrical installation
- Enable adjunct systems

This completes the upgrade procedures.

Chapter 10: Manual upgrade of an S8300A and G700 to R4.0

About upgrading an S8300A to R4.0

This chapter covers the procedures to upgrade the Communication Manager software, from release 1.2, 1.3, or 2.0, on an installed Avaya S8300 Media Server, version A, to release 4.0 on an S8300 Media Server, version B or C. The procedures to upgrade the G700 firmware use CLI commands instead of the Upgrade Tool. These procedures require replacing version A of the S8300 with version B or C. This chapter also covers the procedures to upgrade the firmware on an installed Avaya G700 Media Gateway.

Important:

This chapter assumes that the currently installed S8300 is version A with Communication Manager release 1.2 or higher. If the currently installed S8300 is version B, follow the upgrade procedures in [Chapter 11: Manual upgrade of an existing S8300B or S8300C and G700 to R4.0](#). If the currently installed release of Communication Manager is release 1.1, you must upgrade to release 1.3 before upgrading to release 4.0.

The B version of the S8300 shows a "B" on the faceplate (see [Figure 51: S8300 version faceplate \(B version is shown\)](#)) and the C version shows a "C" on the faceplate, but the version is not indicated on the faceplate of the A version.

Figure 51: S8300 version faceplate (B version is shown)



The S8300 version can also be determined with the SAT command, `list config all`. The B version is listed as **S8300B**. The C version is listed as **S8300C**. The A version is listed as **S8300**.

The S8300 can be configured as either the primary controller or as a local survivable processor (LSP). When the S8300 is an LSP, the primary controller running Avaya Communication Manager can be either another S8300 or an Avaya S8400, S8500, or S8700-series Media Server.

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

- The version of Communication Manager running on the LSP must be the same as, or later than, the version running on the primary controller.
- If upgrading both the primary controller and the LSP, the LSP must be upgraded first. Then, with Communication Manager turned off on the LSP, the primary controller is upgraded.
- Do not save translations on an LSP.



CAUTION:

These upgrade procedures require remastering the hard drive on the S8300B or S8300C. This can result in a service interruption of 3–4 hours, or up to 6 hours if IA770 is being used.



Tip:

You may skip some of the procedures described in this chapter depending on the upgrade scenario. Watch for the **skip to** instructions.

Issues for IA770 INTUITY AUDIX on Release 1.3 or earlier on an S8300A Media Server



CAUTION:

Communication Manager Release 4.0 does not support the CWY1 integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current IA770 integration administration before the upgrade and then administer the integration to H.323 after the upgrade.

For an upgrade of Communication Manager from Release 1.3 or earlier on an S8300A, the customer must save IA770 administrative data to Mailbox Manager, ASA, or another tool, and restore that data after the upgrade to release 4.0. If administrative data is not saved in another tool, the customer must readminister IA770 INTUITY AUDIX Messaging after the upgrade. Additionally, all names, custom announcements, and messages are lost. Subscribers who use Message Manager should be encouraged to save messages to their personal computers and restore them after the upgrade.

Tasks to upgrade the S8300A to release 4.0 and upgrade the G700 firmware

Before going to the customer site

- [Obtaining a USB DVD/CD-ROM drive](#) on page 544
- [Getting information that the project manager provides](#) on page 544
- [Filling in the EPW, if upgrading from release 1.3 or earlier](#) on page 544
- [Getting the serial number of the G700, if necessary](#) on page 544
- [Checking the number of allocated ports](#) on page 545
- [Checking the availability of the FTP server for backing up data](#) on page 545
- [Obtaining S8300 software and G700 firmware](#) on page 545
- [Obtaining service pack files, if needed](#) on page 546
- [Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary](#) on page 548
- [Completing the RFA process \(obtaining license and password files\)](#) on page 549
- [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 550
- [Ensuring a super-user login exists](#) on page 551
- [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#) on page 553

Preparing for the upgrade to R4.0 on-site

- [Accessing the S8300](#) on page 555
- [Removing the administration for the IA770 integration if CWY1 board is used](#) on page 555
- [Checking current software release](#) on page 556
- [Completing pre-upgrade tasks — if the S8300 is the primary controller](#) on page 557
- [Getting IA770 data and stopping IA770 \(if IA770 is being used\)](#) on page 561
- [Checking for any IA770 custom announcement sets \(R2.0 only\)](#) on page 563
- [Stopping IA770](#) on page 564
- [Backing up system files](#) on page 565
- [Recording configuration information](#) on page 568
- [Installing the pre-upgrade software service pack, if necessary](#) on page 569

Replacing the S8300A

- [Linux migration backup \(if current release is 1.2.0 through 1.3.x\)](#) on page 572
- [Replacing the S8300A with the S8300B or S8300C Media Server](#) on page 575

Installing the S8300B or S8300C Media Server

- [Upgrading the S8300B or S8300C Media Server](#) on page 577
- [Setting telnet parameters](#) on page 577
- [Remastering the S8300 and installing the upgrade software](#) on page 577
- [Verifying software version](#) on page 581
- [Copying Files to the S8300 hard drive](#) on page 581
- [Downloading optional language files, if needed](#) on page 583
- [Installing security and Communication Manager service pack updates, if any](#) on page 583
- [Setting the Time, Date, and Time Zone](#) on page 585
- [Configuring network parameters](#) on page 585
- [Verifying connectivity](#) on page 588
- [Disabling RAM disk on the media server](#) on page 588
- [Rebooting the media server](#) on page 588
- [Restoring data backup](#) on page 589
- [Enabling RAM disk on the media server](#) on page 593
- [Rebooting the media server](#) on page 593
- [Installing updated license and authentication files](#) on page 594
- [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 596
- [If the server is an LSP, stop and start Communication Manager](#) on page 599
- [Verifying media server configuration \(Release 1.2 or later\)](#) on page 600
- [If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started](#) on page 601
- [Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary](#) on page 602
- [Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary](#) on page 602
- [Saving translations](#) on page 603

Upgrade the firmware on the G700 Media Gateway

- [Verifying the contents of the tftpboot directory](#) on page 604
- [Determining which firmware to install on the G700](#) on page 605
- [Installing new firmware on the P330 Stack Processor](#) on page 606
- [Installing new firmware on the G700 Media Gateway Processor](#) on page 607
- [Installing new firmware on the media modules](#) on page 609
- [Setting rapid spanning tree on the network](#) on page 611
- [Installing new firmware on other G700 media gateways](#) on page 612

Post-upgrade tasks

- [Stopping IA770 INTUITY AUDIX Messaging, if installed](#) on page 613
- [Installing IA770 service pack \(or RFU\) files, if any](#) on page 614
- [Starting IA770 INTUITY AUDIX Messaging, if installed](#) on page 614
- [Verifying start up of IA770 INTUITY AUDIX Messaging, if installed](#) on page 615
- [Saving translations](#) on page 616
- [If using IA770, administering switch integration for H.323](#) on page 616
- [Administering IA770 \(Release 1.3 or earlier\)](#) on page 616
- [Testing to verify system functionality](#) on page 616
- [To check media modules](#) on page 617
- [To enable scheduled maintenance](#) on page 617
- [To busy out trunks](#) on page 617
- [To check for translation corruption](#) on page 617
- [To resolve alarms](#) on page 617
- [To re-enable alarm origination](#) on page 618
- [To back up the system](#) on page 618
- [To restart LSPs \(if any\)](#) on page 618

Before going to the customer site

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

Obtaining a USB DVD/CD-ROM drive

Upgrading Communication Manager on an S8300 to release 4.0 requires remastering the S8300B/C hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD/CD-ROM drive at the site.

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Filling in the EPW, if upgrading from release 1.3 or earlier

If you are upgrading from release 1.3 or earlier, you will need to do a complete configuration of the S8300B or C after the upgrade to release 4.0. The most efficient way to do this is to fill in the Electronic Pre-installation Worksheet (EPW) and use the Avaya Installation Wizard to complete the server configuration task. You should download the latest version of the EPW from <http://support.avaya.com/avaya/iw/> to your laptop. You can fill in most or all of the configuration information before going to the site. Any missing information can be added to the EPW at the site by viewing the configuration screens using the Maintenance Web Interface before the upgrade.

Getting the serial number of the G700, if necessary

To create a new license file or update an existing license file, you need the serial number of the G700 in which the S8300 is installed.

For an upgrade of an installed S8300, the existing license file can usually be reused. However, if the customer is adding feature functionality (for example, adding BRI trunks), or if the upgrade is between major releases (for example, 1.3 to 2.1), you will need an updated license file. To get the serial number of the G700, ask the customer's administrator to log into the S8300 web page and select **View License Status** from the main menu to display the serial number. The serial number should also be on a sticker on the back of the G700 chassis but this number is occasionally incorrect.

Checking the number of allocated ports



CAUTION:

Release 4.0 of Communication Manager supports a maximum of 900 ports if the S8300 is a primary controller. If the existing system has more than 900 ports allocated, then there may be a problem with the upgrade and you need to escalate.

To check the system for the maximum number of ports

1. Type the SAT command, `display system-parameters customer options` and press **Enter**.
2. Verify that the **Maximum Ports:** field is 900 or less.

Checking the availability of the FTP server for backing up data

During the installation and upgrade procedures, you must back up the system data to an FTP server. You use a server on the customer's LAN for backups. A current version of the system data is required to restore the system configuration upon completion of the upgrade.

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



Important:

Before going to the customer site, make sure that you can use a customer server over the LAN for backups.

Obtaining S8300 software and G700 firmware

The files containing the software for the S8300 and the G700 and media module firmware are on the Communication Manager Software Distribution CD-ROM that you take to the site. This CD is called the software CD because it contains software for all of the Linux servers.

Additional files that may be needed are:

- License file
- Authentication file
- Software service pack files (most recent version)

- Security update files
- G700 firmware file (most recent version)

Obtaining service pack files, if needed

Table 36: R4.0 Upgrade requirements depending on pre-upgrade release

Software Release Before Upgrade to Release 4.0	Upgrade Requirement
Release 1.2.x, 1.3.1. R011x.02.110.4 R011x.03.526.6	You must apply a pre-upgrade service pack to the system files before backing up the system and translations files using Linux Migration Backup/Restore (LMBR). Once the hard drive is remastered and the new software is installed on the S8300B or C, you can restore all the files using LMBR ¹ .
Release 1.3.1.x R011x.03.1.531.0 R011x.03.1.5xx.x	No pre-upgrade service pack required. Back up the system and translations files using Linux Migration Backup/Restore (LMBR). Once the hard drive is remastered and the new software is installed on the S8300B or C, you can restore all the files using LMBR.
Release 2.0.x R012x.00.0.000.0 R012x.01.x.xxx.x	No pre-upgrade service pack is required for the Linux backup. Back up the system and translations files using Data Backup/Restore ² . Once the hard drive is remastered and the new software is installed on the S8300B or C, you can restore the files using Data Backup/Restore.

1. The LMBR backup contains backup sets for the translations, OS and system files.

2. The Data backup contains backup sets for the translations, OS and system files, security files, and AUDIX data, if any.

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

Service packs may or may not be needed, depending on the release of Communication Manager. For both new installations and upgrades, you may need to install a service pack after the installation or upgrade. For an upgrade, you may need a service pack before the upgrade as well.

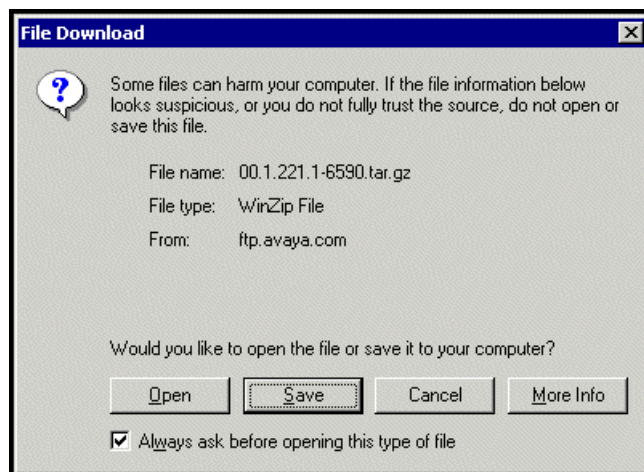
To download a service pack

1. On your laptop, create a directory to store the file (for example, c:\S8300download).

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

The File Download window displays.

File download window



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

To upgrade from release 1.2.x or 1.3.0

1. If you are upgrading from release 1.2.x or 1.3.0, on the **Document Preview/Software Updates** page, locate the service pack file name that matches the load currently installed on the system you are upgrading.

The file name ends with .tar.gz (*for example*, if upgrading from 1.3, the filename will be similar to 03.1.661.5-1003.tar.gz).

2. Double-click the file name.

The system displays a **File Download** window.

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

Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary

If IA700 is installed, determine whether a service pack is needed and/or optional languages are used.

Checking the size of stored messages (CM 2.0 only)

To check the size of stored messages:

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **System Configuration and Status > System Status**.
3. Look for "Used Hours of Speech" in the list.

If more than 72 hours is reported, the customer must delete some messages before the upgrade. Or, you can enter the Linux CLI command,

```
/vs/bin/util/vs_status.
```

Obtaining an IA770 service pack file

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file can be found on the Avaya Support Web Site at <http://support.avaya.com>.

To obtain an IA770 service pack file

1. On the Avaya Support Web site, click on **Find Documentation and Downloads by Product Name**.
2. Under the letter "I", select **IA 770 INTUITY AUDIX Messaging Application**.
3. Click on **Downloads**.

To download the IA770 patch software:

4. Click on **IA 770 INTUITY AUDIX Embedded Messaging Application Patches**.
5. Click on the service pack file name for this release.

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

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

Note:

The IA770 patch documentation is co-located with the patch software.

Obtaining optional language files

Optional languages are any language other than English (***us-eng*** or ***us-tdd***). If optional languages are used with this IA770, you will download the appropriate language files from a language CD after the upgrade. The customer should have the language CD(s) at the site. If not, you need to obtain the appropriate language CD(s) and take them to the site.

Completing the RFA process (obtaining license and password files)

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

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

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

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

Note:

For an upgrade, you do not normally need to install a new authentication file (with a .pwd extension). However, if one is required, follow the same steps as with a license file.

Downloading license file and password for an LSP

The license file of the S8300 as a Local Survivable Processor must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300, S8400, S8500, S8700, S8710, or S8720). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

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

Note:

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

To download the license and password files to your laptop



Tip:

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

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and password files (for example, C:\licenses).
2. Access the Internet from your laptop and go to Remote Feature Activation web site, rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and password files for the customer.
4. Check that the license and password files are complete.
You might need to add the serial number of the customer's G700.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and password files to your laptop.

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

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

Note:

Business Partners call 800-295-0099. ART is available only to Avaya associates.

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

Note:

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

To run the ART

1. Access the ART web site on your laptop at <http://art.dr.avaya.com>.
2. Select **Administer S8x00 Server products for installation script**.
 - a. Log in.
 - b. Enter the customer information.
 - c. Select **Installation Script**.
 - d. Click **Start Installation script & IP Addr Admin**.A script file is created and downloaded or emailed to you.
3. You can use the installation script to set up an IP address and other alarming parameters automatically.

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

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

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

Ensuring a super-user login exists

A super-user login must be administered prior to upgrading the S8300 Media Server. The project manager, remote services, or the customer should check to verify that one exists. If a super-user login must be added, you must log in as *dadmin* or a higher level of login. For pre-4.0 releases, you cannot add the login by logging in as *craft*.

**Important:**

The Communication Manager Web pages for the upgrade might time out if too much time elapses without activity. In this case, you might not be able to log in again with the craft login. This problem can occur after you install the new media server and restore translations and security files, but *before* you install the new authentication file. In such a case, you also cannot login with other higher-level services logins such as INADS. However, you *can* relogin with the customer's super-user login, if it exists. Then you can install the new authentication file and complete the upgrade.

Therefore, it is critical that you ensure that a super-user login exists before you perform the upgrade. In addition, you should retrieve the super-user login and password from the customer prior to performing the upgrade.

Checking a pre-4.0 release

To ensure that a super-user login exists in Communication Manager prior to Release 4.0:

1. Log in with **telnet**.
2. At the SAT command line, enter **list logins**

The Logins screen appears.

list logins									
			LOGINS						
Login	Service Level	Status	Pwd. Cycle	Aging (Days)	ASG	Blk	Expiration Date	No. of Sess. Sess.	Used
init	init	active			y	n	/ /		
inads	inads	inactive			y	n	/ /		
dadmin	dadmin	inactive			n	n	/ /		
craft	craft	inactive			y	n	/ /		
acpsnmp	non-super-user	void			n	n	/ /		

3. Under the Service Level column, look for a login that has either the dadmin or super-user level.
4. If a super-user login does not exist, create one. See [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#).

Creating a super-user login, if one does not exist (releases earlier than Release 4.0)

If a super-user login does not exist, one must be added before you can complete the upgrade. The customer or remote services should complete the following task.

1. Use the following steps only if you are starting from a software release *earlier* than Release 4.0:

Note:

Adding a super-user login with the SAT command line requires a dadmin, init, or inads login.

Note:

If you are upgrading an S8300 LSP, create the super-user login on the primary controller using this procedure. Then, at the Llinux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

2. At the SAT command line, enter add login.

The Login Administration screen appears.

add login
Page 1 of x

LOGIN ADMINISTRATION

Password of Login Making Change:

LOGIN BEING ADMINISTERED

Login's Name:xxxxxxx

Login Type:

Service Level:

Disable Following a Security Violation?

Days to Disable After Inactivity:

Access to INADS Port?

LOGIN'S PASSWORD INFORMATION

Login's Password:

Reenter Login's Password:

Password Aging Cycle Length (Days):

LOGOFF NOTIFICATION

Facility Test Call Notification?

Acknowledgment Required?

Remote Access Notification?

Acknowledgment Required?

ACCESS SECURITY GATEWAY PARAMETERS

Access Security Gateway?

3. In the **Password of Login Making Change** field, type your password.

4. In the **Login's Name** field, type a login name agreed upon with the customer. Alternatively, a Business Partner may add the dadmin login.
5. In the **Login Type** field, type **customer**.
6. In the **Service Level** field, type **super-user**.
7. In the **Days to Disable After Inactivity** field, type **90**.
8. In the **Login's Password** field, type a password.
9. In **Reenter Login's Password** field, type the password again.
10. In the **Password Aging Cycle Length** field, type 90, and press **Enter**.
11. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.
 - a. Log in with `telnet`.
 - b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

Preparing for the upgrade to R4.0 on-site

When you arrive on-site, you must perform the following tasks in preparation for the upgrade to release 4.0.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See [Laptop configuration for direct connection to the services port](#) on page 42.

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

- [Accessing the server's command line interface with SSH](#) on page 55
- [Logging in to the media server from your laptop using Telnet](#) on page 56
- [Logging in to the S8300 Web Interface from your laptop](#) on page 57

Removing the administration for the IA770 integration if CWY1 board is used

Note:

If the S8300 is configured as an LSP, skip to [Checking current software release](#) on page 556.



CAUTION:

Communication Manager Release 4.0 does not support the CWY1 method of integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current switch integration administration now. You will administer the integration for H.323 after the upgrade.

For instructions on removal of existing CWY1 administration, see *Administering Media Servers to work with IA770*.

Note:

For Releases 2.0 and earlier of Communication Manager that use IA770, you *cannot* remove messaging from the Media Gateway screen in the SAT interface *before* the upgrade. Therefore, you must remove messaging from Slot V8 of the Media Gateway screen after the upgrade, then administer the H.323 integration.

Checking current software release

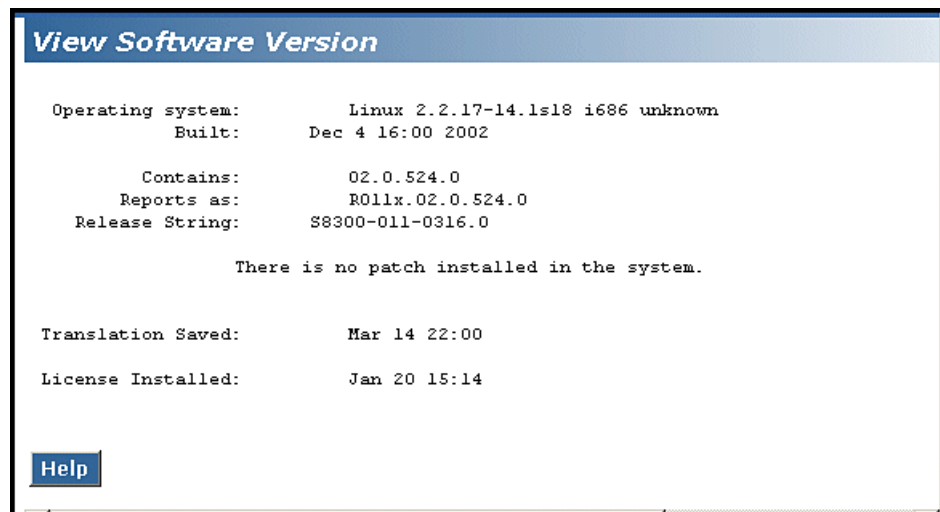
Check the release of Communication Manager currently running on the S8300 to determine whether a pre-upgrade service pack is required.

To check the current software release

1. Log in to the Web interface on the S8300 and launch the Maintenance Web Interface.
2. Choose **View Software Version** under Server Configuration and Upgrades.

The system displays the **View Software Version** screen.

Software Version Screen



3. Check the **Reports as:** field for the release number of the S8300 software.

In this example, the release number is reported as R011x.02.0.524.0. This corresponds to release 1.2.0. [Table 37](#) maps the release number to the **Reports as:** field, and specifies whether or not a pre-upgrade update is required.

Table 37: Software Release Numbers

Release Number Reported as	Release Number	Pre-upgrade update Required?
From: R011x.01.0.xxx To: R011x.01.9.xxx	1.1.0 to 1.1.9	No, but requires an upgrade to 1.3
From: R011x.02.0.xxx To: R011x.03.0.xxx	1.2.0 to 1.3.0	Yes
From: R011x.03.1.xxx To: R011x.03.9.xxx	1.3.1 to 1.3.9	No
From: R012x.00.0.xxx To: R012x.00.9.xxx	2.0.0 to 2.0.9	No

Completing pre-upgrade tasks — if the S8300 is the primary controller

Skip to [Backing up system files](#) on page 565, if the S8300 is configured as an LSP.



CAUTION:

If you are upgrading an S8300 primary controller that has LSPs registered to it, the LSPs must be upgraded **before** the primary controller. (You can use the SAT command, list media-gateway, to see if there are LSPs registered to the S8300.)

Perform the following procedures if you are upgrading an S8300 that is configured as a primary controller:

- [To display IA770 alarms, if IA770 is enabled](#)
- [To clear alarms](#)
- [To check link status](#)
- [To record all busyouts](#)
- [To disable scheduled maintenance](#)
- [To check for translation corruption](#)
- [To save translations](#)
- [To stop Communication Manager on an LSP](#)
- [To disable alarm origination](#)

Note:

It is no longer necessary to disable Terminal Translation Initialization (TTI) before an upgrade or to enable it after an upgrade.

To display IA770 alarms, if IA770 is enabled

1. On the Maintenance Web Interface, click **Messaging Administration**.
2. On the Messaging Administration menu, under Logs, click **Alarm**.
3. On the Alarm Log screen, type today's date. Leave the defaults in all other fields.
4. Click Display.
5. Resolve any alarms that are listed.

To clear alarms

1. On the Maintenance Web Interface under Alarms, click **Current Alarms**.
2. If no alarms are listed, skip the next two steps.
3. If alarms are listed, click **Clear All**.
4. Resolve any remaining major alarms through the Communication Manager SAT.

To check link status

1. Open a SAT session.
2. Enter `display communication-interface links`.
Note all administered links.
3. Enter `status link number` for each administered link.

4. Enter `list signaling group`.

Note the signaling groups listed by number.

5. For each of the signaling groups listed, enter `status signaling group number`.

Make a note (write down) of any links that are down.

To record all busyouts

1. At the SAT prompt, type `display errors` and press **Enter**.
2. Look for type 18 errors and record (write down) any trunks that are busied out — you will return them to their busy-out state after the upgrade.

To disable scheduled maintenance

Scheduled daily maintenance must not interfere with the upgrade.

1. At the SAT prompt, type `change system-parameters maintenance` and press **Enter**.
2. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

or,

If scheduled maintenance is not in progress, set the **Start Time** field to a time after the upgrade will be completed.

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

To check for translation corruption

1. At the SAT prompt, type `newterm` and press **Enter**.
2. Enter your terminal type and press **Enter**.

If you see the message,

Warning: Translation corruption found

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To save translations

1. At the SAT prompt, type `save translation` and press **Enter**.
2. Under **Command Completion Status** you should see `Success`.

To stop Communication Manager on an LSP

Skip this procedure if no LSPs are registered to the S8300.

For configurations with LSPs, the LSPs can run the same version or a later version of Communication Manager than the version running on the primary controller. Normally, the primary controller and the LSPs should run the same version of Communication Manager. Therefore, an upgrade to an LSP is usually accompanied by an upgrade of the primary controller.

Note:

You should upgrade the LSP **before** you upgrade the primary controller.

Before you upgrade the primary controller, you need to shut down Communication Manager on the LSPs. This prevents the phones and other endpoints attached to the G700 from trying to register with the LSPs while you are upgrading the primary controller.

1. Open a telnet session on the S8300 (LSP).
2. Telnet to the LSP.
3. At the command line, type **stop -acfn** and press **Enter**.

The S8300 (LSP) shuts down Communication Manager.



CAUTION:

The LSP's Communication Manager must remain shut down while you upgrade the primary controller. When you complete the primary controller upgrade, run **save translation** on the primary controller before restarting Communication Manager on the LSP. The save translations process will automatically cause the G700's endpoints to reregister with the primary controller.

After the primary controller has been upgraded, you need to restart the LSPs.

To disable alarm origination

If alarm origination is enabled during the upgrade, unnecessary alarms will be sent to the Operations Support System (OSS) destination number(s). Even if you selected **Suppress Alarm Origination** when you logged in, alarm origination will be automatically re-enabled when the system reboots after the software upgrade. Use this procedure to prevent alarm origination from being re-enabled after reboot.



CAUTION:

If you do not disable alarm origination, the system can generate alarms during the upgrade, resulting in unnecessary trouble tickets.

1. Logoff the SAT session.
2. At the command prompt, type **almenable -d n -s n**, where
 - d n sets the dialout option to **neither** (number)
 - s n disables SNMP alarm origination

Note:

Be sure to reset alarm origination after the upgrade.

3. Type **almenable** (without any options) to verify the alarm origination status.

You should see:

```
incoming: enable
```

```
Dial Out Alarm Origination: neither
```

```
SNMP Alarm Origination: n
```

Getting IA770 data and stopping IA770 (if IA770 is being used)

Skip to [Backing up system files](#) on page 565 if IA770 is not being used.

If IA770 is being used, you need to collect data, leave a test message, and shut down IA770 before backing up the files.

Creating an IA770 test message (R2.0 only)

To test IA770 after the migration

1. Write down the number of a test voice mailbox, or create one if none exists.
2. Write down the number of the IA770 hunt group.
3. Leave a message on the test mailbox that will be retrieved after the migration.

Determining whether optional languages are needed

To determine the system language

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Global Administration** then **Messaging Administration**.
3. Enter the *craft* password.
4. At the command prompt, enter **display system-parameters features**.
The **System-Parameters Features** screen displays.
5. Go to page 3.

System-Parameters Features screen

```

redtail          Active          Alarms: none          Logins: 1
display system-parameters features          Page 3 of 4
SYSTEM-PARAMETERS FEATURES

CALL TRANSFER OUT OF AUDIX
Transfer Type: enhanced_cover_0          Transfer Restriction: digits
Covering Extension: 50104

ANNOUNCEMENT SETS
System: us-eng          Administrative:

RESCHEDULING INCREMENTS FOR UNSUCCESSFUL MESSAGE DELIVERY
Incr 1: 0 days 0 hrs 5 mins          Incr 2: 0 days 0 hrs 15 mins
Incr 3: 0 days 0 hrs 30 mins          Incr 4: 0 days 1 hrs 0 mins
Incr 5: 0 days 2 hrs 0 mins          Incr 6: 0 days 6 hrs 0 mins
Incr 7: 1 days 0 hrs 0 mins          Incr 8: 2 days 0 hrs 0 mins
Incr 9: 7 days 0 hrs 0 mins          Incr10: 14 days 0 hrs 0 mins

enter command: display system-parameters features
Cancel Refresh Enter ClearFld Help Choices NextPage PrevPage

```

6. Under **Announcement Sets**, note the main system language listed after **System**:

In this example, the main system language is English (**us-eng**). If the system language is anything other than us-eng or us-tdd, you will need to download the appropriate language files from a language CD after the upgrade. Also, for Release 2.0 only, if the language is a custom set, you must change the name to **us-eng** or **us-tdd**. See [Checking for any IA770 custom announcement sets \(R2.0 only\)](#) on page 563.

Note:

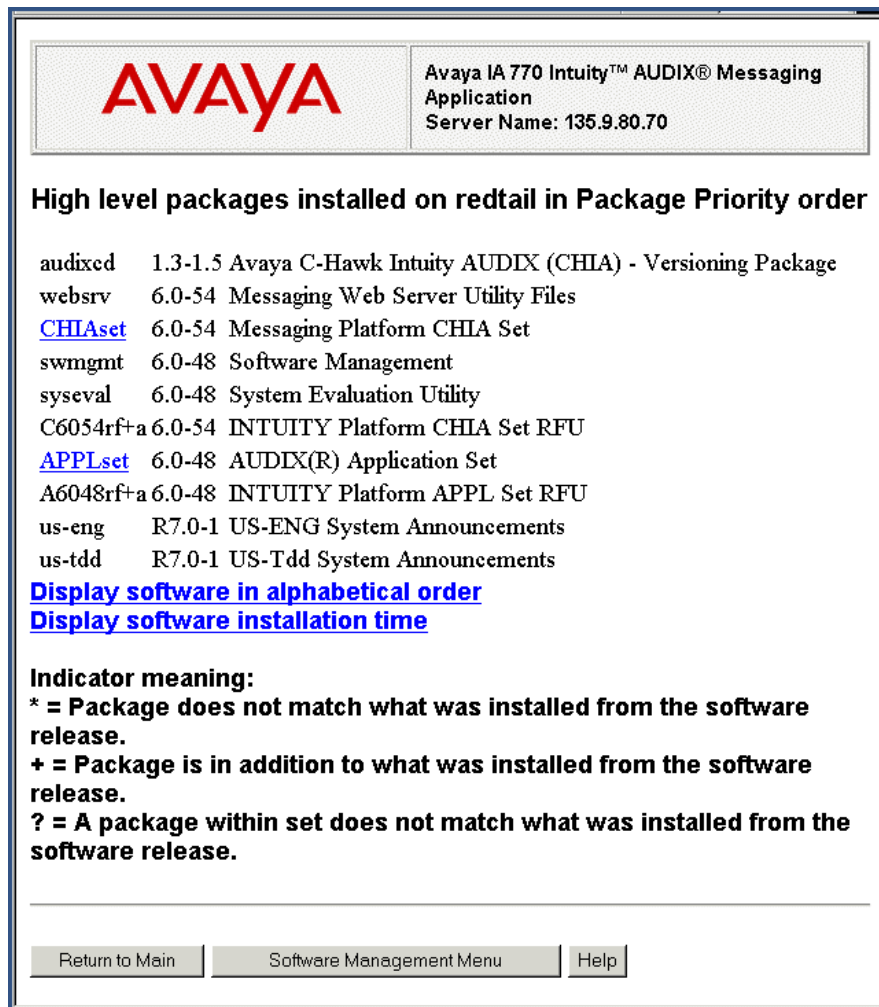
Starting with release 2.1, only English language files (us-eng and us-tdd) are included with the Communication Manager software. Before release 2.1, Latin American Spanish and Canadian French (lat-span and french-c) were also included.

7. Press **F1** to cancel the command.
8. Type **exit** and press **Enter** to close the CLI interface.
9. Click on **Main Menu** to return to the Maintenance Web Interface.

To identify other needed languages

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Utilities**, then **Software Management**, then **Messaging System Software Display**. The **IA770 Messaging Application** screen displays.

IA770 Messaging Application screen



3. Note the **System Announcements** language files listed.

In this example, **us-eng** and **us-tdd** are listed. If Latin-Spanish (**lat-span**) and Canadian French (**french-c**) are listed, ask if these will be used with the release 4.0 system. If any other language files are listed, you will need to download the additional language files from a language CD after the upgrade.

Checking for any IA770 custom announcement sets (R2.0 only)

When you restore announcement sets, Communication Manager looks for standard names for the announcement sets. Therefore, if a custom announcement set exists, check with the customer to ensure that the customer wants to restore it. If the set is to be restored, you must change the name of the set to a standard name, either **us-eng** or **us-tdd**.

In this case, do the following:

1. Add a name for the standard announcements backup set, for example, us-eng-backup.
2. Copy the standard announcements from the standard set, for example us-eng, to the backup set.
3. Copy the announcements of the custom announcement set into the announcement set with the standard name.

Stopping IA770

To stop IA770:

1. Type `telnet 192.11.13.6` and press **Enter**.
2. Log in as *craft* or *dadmin*.

Note:

You must enter the commands in the next two steps using upper-case as indicated.

3. Type `stop -s Audix`, and press **Enter** to shut down AUDIX. Note that the "A" in Audix must be capitalized.

The shutdown takes a few minutes.

4. Type `watch /vm/bin/ss`, and press **Enter** to monitor the shutdown.

The watch command automatically refreshes every few seconds. When the shutdown is complete, you see only the voicemail and audit processes. For example:

```
voicemail: (10)
```

```
audit http: (9)
```

Press **Ctrl+C** to break out of the `watch` command.

5. Type `/vs/bin/util/vs_status`, and press **Enter** to verify that AUDIX is shut down.

When AUDIX is shut down, you see the message

```
Voice System is Down.
```



Important:

After upgrading an S8300 media server, you must upgrade the G700 or G350 media gateway firmware and media module firmware before restarting IA770.

Backing up system files

For releases 1.2.0 through 1.3.9, this backup is optional but recommended in case there is a need to back out of the upgrade.

**CAUTION:**

If the current release of Communication Manager is 2.0.x, you **must** use this procedure to back up system, security, and translations data (including AUDIX data if IA770 is installed). For these releases, you will restore some or all of the backup sets after the upgrade.

To perform a backup, you need an FTP address, directory path, and a user ID and password to access an FTP server on the customer's network. Check with your project manager or the customer for this information.

To back up data

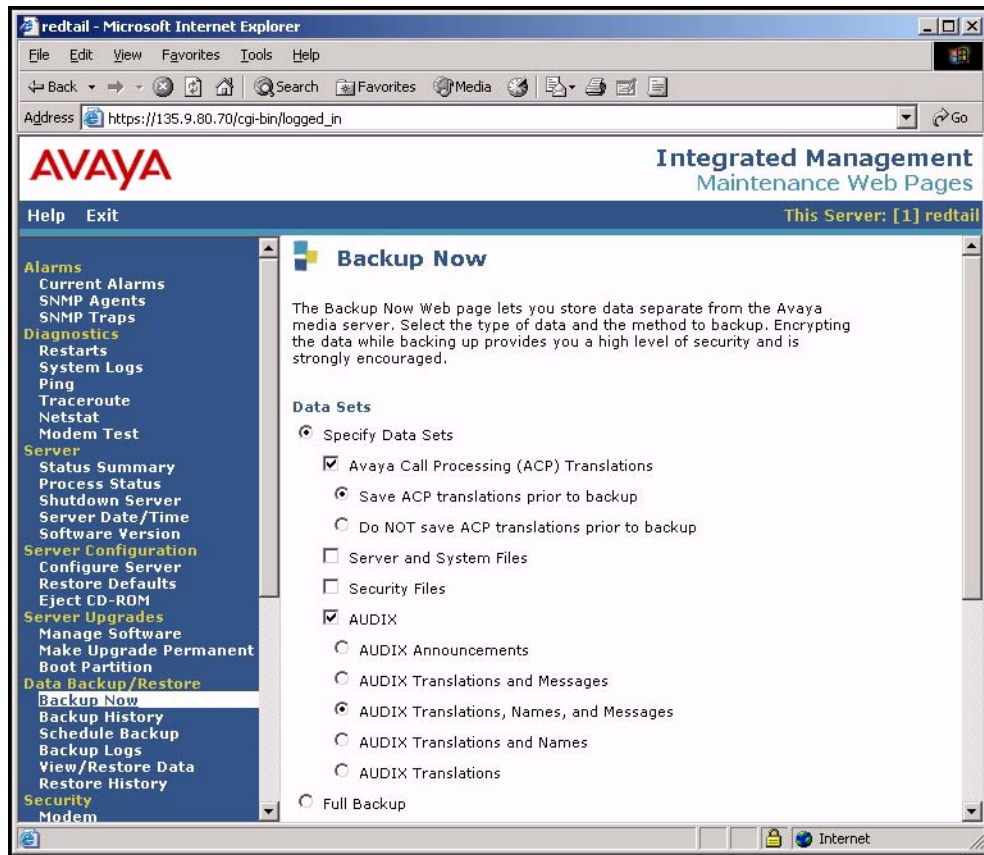
1. On the Maintenance Web Interface under Data Backup/Restore, click **Backup Now**.

The **Backup Now** screen displays.

**Tip:**

Depending on the Communication Manager software version, the following screen may look slightly different.

Backup Now screen (Part One)



2. Select all data sets:

- Avaya Call Processing (ACP) Translations
- Save ACP translations prior to backup

Note:

Select ACP translations only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

- Server and System Files
- Security Files

3. If the AUDIX options are available, select AUDIX and select AUDIX Translations, Names, and Messages.

Backup Now screen (Part Two)

4. Select **FTP** for the backup method.

Fill in the User Name, Password, Host Name, and Directory fields with information provided by the customer.

5. Click **Start Backup** to back up the files.

Note:

The backup and restore processes use the ping service to check connectivity to the backup server. If a backup or restore operation fails, ensure that the ping service is enabled:

- i. On the Maintenance Web Interface, under Security, select **Firewall**.
- ii. In the Service column, find ping.
- iii. The checkboxes for both **Input to Server** and **Output from Server** should be checked.

6. To check the status of the backup,
 - a. Click **Backup History** on the main menu.
 - b. Select the backup set and click **Check Status**.

You can click **Refresh** to update the screen while the backup is running.

7. When the backup is finished, you will see

The final status for your backup job is shown below

on the **Backup History Result** screen. Check for any errors reported on this screen. You should see a **Success** message for each backup set.

8. If the AUDIX options are available, repeat Steps 3–7 for AUDIX Announcements.

Recording configuration information

If you have not already done so, you must record the current server configuration data, which will be re-entered after the upgrade. If you are upgrading from release 1.1, most of the configuration data will be re-entered automatically with the restore process. However, if you are upgrading from a 1.2 release, you will need to re-enter all of the server configuration data.

To view and record the current configuration data

1. Launch the Maintenance Web Interface.
2. Under Server Configuration and Upgrades, click **Configure Server**.
3. Click **Continue** on the first and second screen.
4. On the **Select method for configuring server** screen, select **Configure all services using the wizard** and click **Continue**.
5. View and record the configuration information on each screen, and click **Continue** to move to the next screen.
6. When you get to the **Update System** screen, click **Cancel**.

The best way to record the configuration data is to fill in the Electronic Pre-installation Worksheet (EPW). You then have the option to use the Installation Wizard to do the server configuration task. If you do not have the EPW, you can record the current configuration data and enter it manually after the upgrade.

1. If upgrading from 1.2 or later, record the Host name displayed on the **Configure Server** screen.
2. On the **Configure Interface** screen, record the following data:
 - Server IP address
 - Gateway IP address,
 - Subnet mask
 - Integrated Messaging IP address, if configured

You can skip the remaining configuration screens.

3. If upgrading from the 1.1 release, record the data from all configuration screens.

Replacing the S8300A

**CAUTION:**

This upgrade procedure, including remastering the hard drive on the S8300, requires a service interruption of approximately 4 hours, or up to 6 hours if IA770 is being used.

This section describes the procedures for upgrading the S8300A Media Server from a pre-2.2 release of Communication manager to release 4.0.

Upgrading an S8300 to release 4.0 requires removing the S8300A and replacing it with an S8300B or C. The remastering program on the software distribution CD remasters the hard drive and installs the R4.0 Communications Manager software. These procedures are described in this section.

Installing the pre-upgrade software service pack, if necessary

A pre-upgrade service pack is required only if the current software is between **1.2.0** and **1.3.0**.

If the current software release is between **2.0.0** and **2.0.9**, skip this service pack installation procedure and go to [Replacing the S8300A with the S8300B or S8300C Media Server](#) on page 575.

If the current software release is **1.3.1**, skip this service pack installation procedure and go to [Linux migration backup \(if current release is 1.2.0 through 1.3.x\)](#) on page 572.

Note:

Typically, any existing service pack(s) should be removed before installing a new service pack. However, removing existing service packs is not necessary for this procedure.

To copy pre-upgrade service pack file to the media server

1. Make sure the software CD is in the CD-ROM drive of your laptop.
2. On the Maintenance Web Interface, under Miscellaneous, click **Download Files**.
3. Select the download method, "Files to download from the machine I'm using to connect to the server."

Note:

Do not select the checkbox, "Install this file on the local server."

4. Browse to the directory on the software CD (or laptop) that contains the pre-upgrade service pack file.
5. Select the pre-upgrade service pack file and click **Download**.

Installing the pre-upgrade service pack

Use *one* of the following two procedures to install the pre-upgrade service pack:

Current release is 1.x, use [To install the pre-upgrade service pack when the current release is pre-2.0.](#) on page 570.

Current release is 2.x, use [To install the pre-upgrade service pack when the current release is 2.x.](#) on page 571.

To install the pre-upgrade service pack when the current release is pre-2.0.

1. Use Telnet to access the media server.
 - a. Click **Start** > **Run** to open the Run dialog box.
 - b. Type `telnet 192.11.13.6` and press **Enter**.
 - c. Log in as *craft*.
2. Type `cd /var/home/ftp` and press **Enter** to access the ftp directory.
3. At the prompt, type `ls -ltr` and press **Enter** to list files in the ftp directory.

The S8300 displays a list of files in the ftp directory.
4. Verify that the directory contains the ***.tar.gz** file you have uploaded.
5. Type `sudo patch_install patch.tar.gz` and press **Enter**.

where *patch* is the release or issue number of the service pack file. (For example, `03.1.526.5-1003.tar.gz`).
6. Type `patch_show` and press **Enter** to list Communication Manager files to verify the new software file was installed.
7. Type `sudo patch_apply patch` and press **Enter**.

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

The media server goes through a software **reset system 4**. You must wait until the restart/reset has completed before entering additional commands. The reset should take 1–2 minutes (or longer if messaging is enabled).
8. Type `patch_show` again and press **Enter** to list Communication Manager files to verify the new software file was applied.
9. Before proceeding, type `statapp -c` to view the status of the processes.

Make sure everything except **dupmgr** shows **UP**. **Communication Manager** should show `65/65 UP` or, if IA770 is installed, `67/67 UP`. To stop the continual refresh of the **statapp** command, type **Ctrl-C**.

Note:

The number of processes (65/65) may vary depending on the configuration. For a normal state, the second number should not be greater than the first number. For example, the numbers 64/65 UP would indicate that a process did not come up and should be investigated before proceeding.

10. Close the telnet session.

To install the pre-upgrade service pack when the current release is 2.x.

Note:

Use a telnet session to install and activate the service pack file.

The following steps activate the service pack.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **telnet 192.11.13.6** and press **Enter**.
3. Log in as either **craft** or **dadmin**.
4. Type **update_unpack** and press **Enter**.
5. Select the number corresponding to the service pack file. (For example, **00.0.339.4-xxxx.tar.gz**). Press **Enter**.
6. Type **update_show** and press **Enter** to list Communication Manager files to verify that the new service pack file was unpacked.
7. Type **update_activate update**, where **update** is the release or issue number of the latest service pack file. (For example, **00.0.339.4-xxxx**. Do *not* use the .tar.gz extension at the end of the file name). Press **Enter**.

The media server may reboot. If it reboots, it also may display the message

```
/opt/ecs/sbin/drestart 2 4 command failed.
```

Ignore this message. You must wait until the restart/reset completes before entering additional commands.

The media server displays a message that the service pack was applied.

8. Type **update_show** again and press **Enter** to list Communication Manager files to verify the service pack file was activated.
9. Enter **y** in response to the question, `Commit this software?`

Linux migration backup (if current release is 1.2.0 through 1.3.x)

 Important:

Skip to [Replacing the S8300A with the S8300B or S8300C Media Server](#) on page 575 if the current software release is 2.x. After the upgrade, you will restore data from the system backup you did earlier.

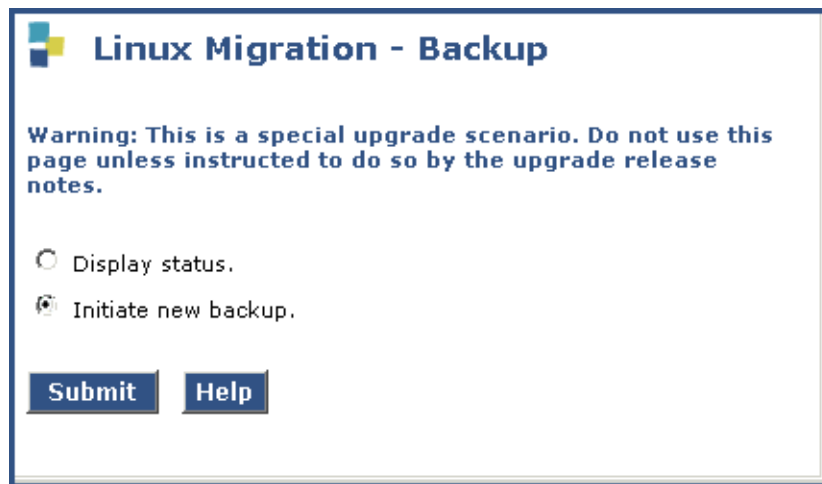
In this section, you will use the Linux Migration Backup procedure on the Maintenance Web Interface to save the system files and translations. After the upgrade, you will use the Linux Migration Restore feature to restore these files.

To perform the Linux migration backup

1. Launch the Maintenance Web Interface. Under Server Configuration click **Linux Migration (Backup/Restore)**.

The **Linux Migration - Backup** screen displays.

Linux Migration - Backup screen



 **Linux Migration - Backup**

Warning: This is a special upgrade scenario. Do not use this page unless instructed to do so by the upgrade release notes.

☐ Display status.

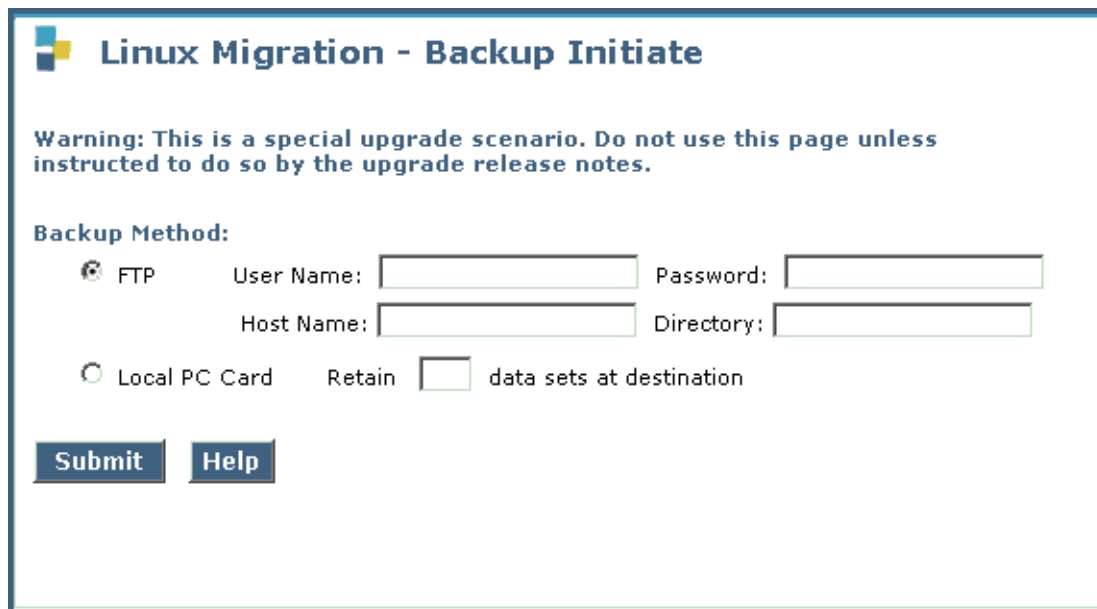
☒ Initiate new backup.

Submit **Help**

2. Select "Initiate new backup or restore" and click **Submit**.

The **Linux Migration - Backup Initiate** screen displays.

Linux Migration - Backup Initiate screen



The screenshot shows a web interface titled "Linux Migration - Backup Initiate". It features a warning message, a "Backup Method" section with radio buttons for "FTP" and "Local PC Card", and input fields for "User Name", "Password", "Host Name", and "Directory". There is also a checkbox for "Retain" and a text label "data sets at destination". At the bottom are "Submit" and "Help" buttons.

Linux Migration - Backup Initiate

Warning: This is a special upgrade scenario. Do not use this page unless instructed to do so by the upgrade release notes.

Backup Method:

☒ FTP User Name: Password:
Host Name: Directory:

☐ Local PC Card Retain ☐ data sets at destination

Submit **Help**

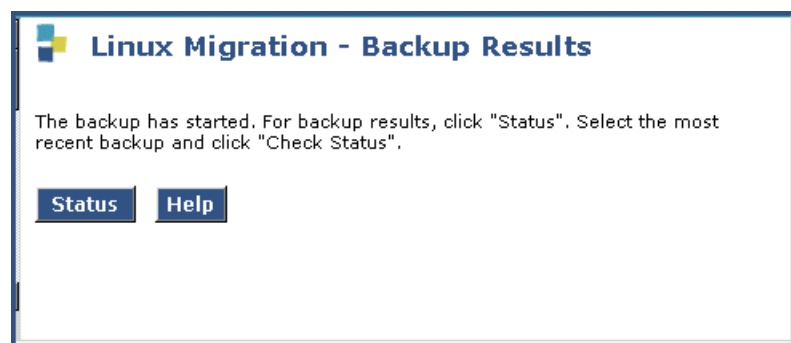
3. Under Backup Method, select FTP

Fill in the **User Name**, **Password**, **Host Name (or host IP address)** and **Directory** fields for the back up location. The backup location should be a server on the customer's LAN.

Click **Submit**.

The **Linux Migration - Backup Results** screen displays.

Linux Migration - Backup Results screen



The screenshot shows a web interface titled "Linux Migration - Backup Results". It contains a message about the backup status and instructions to click "Status" and "Check Status". At the bottom are "Status" and "Help" buttons.

Linux Migration - Backup Results

The backup has started. For backup results, click "Status". Select the most recent backup and click "Check Status".

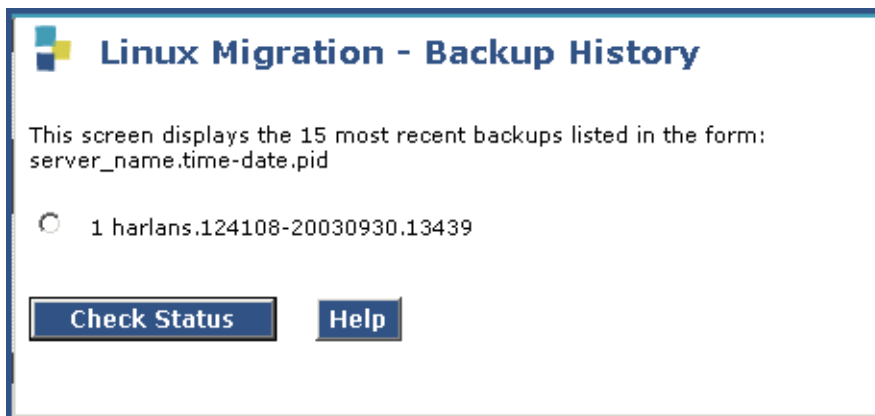
Status **Help**

4. Click **Status** to see the backup progress.

Note:

The Linux Migration backup status function is not enabled for release 1.3.1. To check the backup status when upgrading from 1.3.1, select **Backup Status** under **Data Backup/Restore** on the Maintenance Web Interface menu. The **Linux Migration - Backup History** screen displays. Select the appropriate backup set and click **Check Status**.

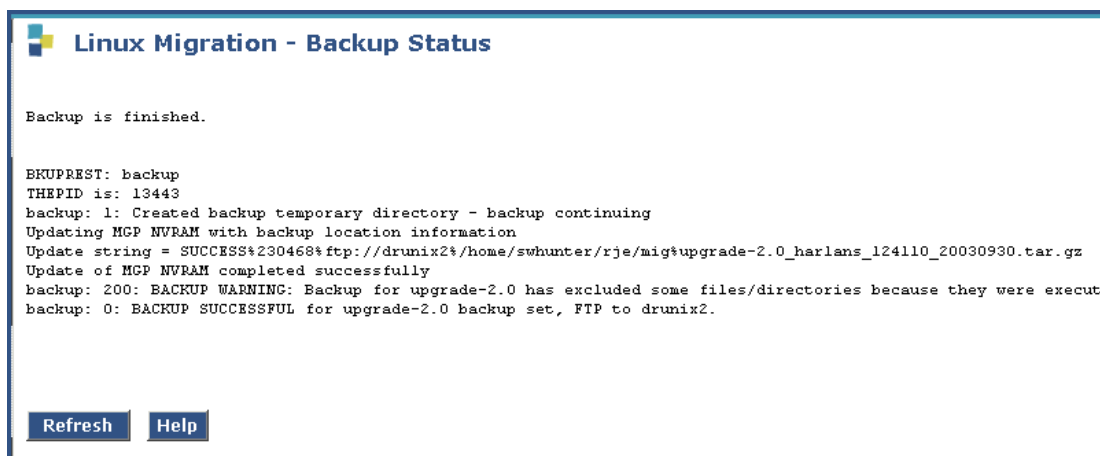
Linux Migration - Backup History screen



5. Select the backup set and click **Check Status** to see the backup results.

If the backup is in progress, click on **Refresh** until the **Backup is finished** message appears.

Linux Migration - Backup Status screen



! CAUTION:

The screen will show **Backup is finished** when the backup is completed. However, also verify that the message, **Backup Successful** also appears in the last line. If any error messages appear stating that the backup failed, follow the normal escalation procedures.

Replacing the S8300A with the S8300B or S8300C Media Server

To remove the S8300A and insert the S8300B or S8300C

1. On the Maintenance Web Interface, under Server select **Shutdown Server**.
2. Select the **Delayed Shutdown** option and **uncheck** the "Restart server after shutdown," checkbox.
3. Click the **Shutdown** button.
Click **OK** to confirm.
4. When the **OK to Remove** LED on the S8300 faceplate goes on steady, it is safe to remove the S8300.



CAUTION:

Be sure to wear a properly grounded ESD wrist strap when handling the S8300 Media Server. Place all components on a grounded, static-free surface when working on them.

5. Loosen the two thumb screws on the S8300 faceplate.
6. When removing or inserting the S8300A circuit pack, the LED module (above slot V1) must also be removed or inserted together with the S8300.

Disengage the LED module and the S8300 circuit pack and remove them together from the G700.

7. If the IA770 INTUITY AUDIX module (CWY1 card) is installed on the S8300B Media Server, leave it on S8300B Media Server.

Note:

The CWY1 card is *not* supported on Communication Manager Release 4.0.

8. Connect the DVD/CD-ROM drive to the new S8300B or S8300C with the following steps:

Note:

You must do this *before* you completely seat the media server in the slot.

- a. Connect the USB cable into one of the USB ports on the faceplate of the S8300.
- b. Connect the other end of the USB cable to the CD-ROM or DVD/CD-RW drive.
- c. If you are using an Addonics DVD/CD-RW drive, connect the power cord to the drive and an electrical outlet.

Note:

The TEAC drive and S8300/S8400 drive get their power from the server over the USB connection.

- d. If you are using an Addonics DVD drive, set the power source switch on the side to **EXT**, not **USB**.
- e. If you are using an S8300/S8400 DVD/CD-RW drive, set the on/off switch to **On**.

Be sure to set the S8300/S8400 drive to **Off** when not in use.

9. Insert the Communication Manager Software Distribution CD in the drive.



CAUTION:

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

Note:

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

10. For an S8300B upgrade, the LED panel (above slot V1) must be reinserted together with the S8300 circuit pack.
 - Insert both the LED panel and S8300 circuit pack about 1/3 of the way into the guides
The guides are in slot V1 for the S8300 and above slot V1 for the LED panel.
 - Push both circuit packs (together) back into the guides, gently and firmly, until the front of each circuit pack aligns with the front of the G700.

For an S8300C upgrade, do the following:

- Reinsert the LED panel (above slot V1) until the front of the panel aligns with the front of the G700.
- Insert the S8300C circuit pack into the slot V1 guides until the front of the circuit pack aligns with the front of the G700.

11. Secure the S8300 faceplate with the thumb screws.

Tighten the thumb screws with a screw driver.

Note:

If the LED panel is not inserted all the way in, all of the status lights (on the left side of the LED panel) will be on. If this is the case, press the LED panel all the way in.

12. Reconnect the laptop to the services port of the new S8300B or S8300C.

Upgrading the S8300B or S8300C Media Server

Setting telnet parameters

The Microsoft Telnet application may be set to send a carriage return (CR) and line feed (LF) each time you press **Enter**. The installation program sees this as two key presses. You need to correct this before you Telnet to the server.

Note:

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

To set telnet parameters

1. Click **Start > Run** to open the Run dialog box.
2. Type `telnet` and press **Enter** to open a Microsoft Telnet session.
3. Type `unset crlf` and press **Enter**.
4. Type `display` and press **Enter** to confirm that **Sending only CR** is set.
5. Type `quit` and press **Enter** to save the setting and close the window.

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

Remastering the S8300 and installing the upgrade software

To begin the upgrade

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.

The first RP screen should display.

The first RP screen



Tip:

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

Note:

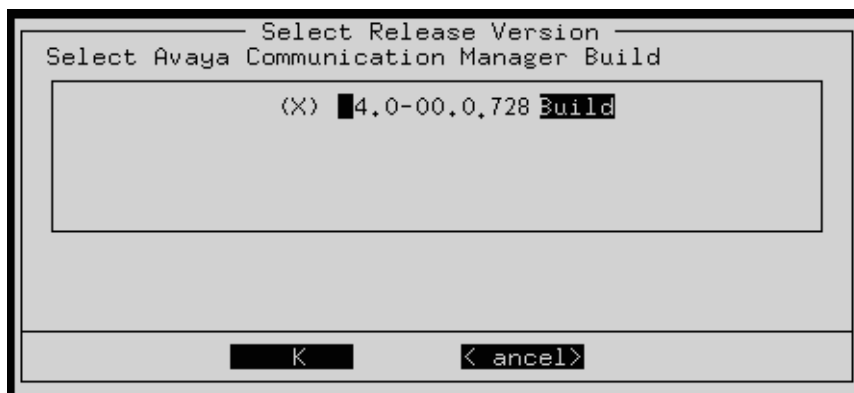
At this point, the installation script looks for the software CD on the DVD/CD drive connected to the USB port. If the DVD/CD drive was not attached to a USB port when the S8300 booted, you will not see any activity on the screen. In this case, perform the following steps:

- Press the Shut Down button on the S8300 Media Server.
- When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port and reseal the S8300 in its slot.

3. Select **Install** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen



4. Select the appropriate release version (if more than one) then select **OK** and press **Enter**.

The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen



5. Select **Yes** if you want to install AUDIX concurrently with Communication Manager. Select **No** if you do not. Then press **Enter**.

Note:

If you do not install IA770 concurrently with Communication Manager at this time, and decide later to install it, you will have to upgrade Communication Manager again (even to the same release). For the upgrade, you use the Manage Software screen on the Maintenance Web interface, and select **Yes** at this screen for IA770 installation.

At this point, the following processes are initiated:

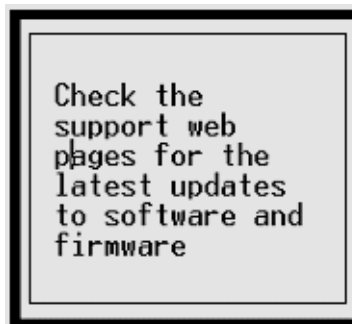
- a. The S8300 hard drive and internal Compact Flash are partitioned and reformatted.
- b. The Linux operating system is installed.
- c. The program begins installing Communication Manager software and reports the progress.

Communication Manager installation progress

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.69-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktmp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

These processes take about 30 minutes. When the media server is ready to reboot, the CD drive door opens and the following screen flashes for about 5 seconds.

Software and firmware update reminder



When the installation is complete, the system reboots automatically and the telnet connection is lost. The reboot takes 1–3 minutes without the IA770 application and 3-6 minutes if the IA770 is present.

6. Click **Start > Run** to open the **Run** dialog box on your laptop.
7. Type `ping -t 192.11.13.6` and press **Enter**.
8. Wait for the reply.

Verifying software version

Note:

Since the system is now running a new software release, you must login with the *initial craft ID and password*. (You cannot use *dadmin* at this point.)

To verify the software version

1. Log in to the Maintenance Web Interface.

See [Logging in to the S8300 Web Interface from your laptop](#) on page 57.

2. Under Server, click **Software Version**.
3. Verify that the media server is running Release 4.0 software.

The **Report as:** string should show **R014x.00** at the beginning of the string. For example, **R014x.00.0.728.0**.

4. Verify that the DVD/CD-ROM drive popped open and disconnect the DVD/CD-ROM drive from the S8300 USB port.

Copying Files to the S8300 hard drive

During reformatting of the hard drive, a new directory, */var/home/ftp/pub*, was created.

You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Post-upgrade software service pack
- License file
- Avaya authentication file
- New firmware files
- Security updates
- IA770 service packs or RFUs

To copy files to the S8300 hard drive

1. Under **Miscellaneous** on the Maintenance Web pages, click **Download Files**.

Download Files screen

Download Files

The Download Files Web page lets you download files to the media server.

☒ File(s) to download from the machine I'm using to connect to the server

☐ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

☐ Install this file on the local server

**If the above box is checked, you may specify only one file for downloading.

2. Select "Files to download from the machine I'm using to connect to the server" and browse to each file you want to copy to the S8300. Leave the "Install this file on the local server" checkbox **unchecked**.

If you need to download an IP Telephone firmware file, download this file last with the "Install this file on the local server" checkbox **checked**.

Note:

To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to `pub` after starting ftp and logging in; that is, type `cd pub`.

3. Click on **Download** to copy the files to the S8300. The transfer is complete when you see the message,

Files have been successfully uploaded to the server



Important:

Remove the Communication Manager software distribution CD from the DVD/ CD-ROM drive.

Downloading optional language files, if needed

If the optional language files are needed, copy the files from the language CD to `/var/home/ftp/pub`.

To download optional language files

1. Insert the optional language CD in your laptop's CD-ROM drive.
2. On the Maintenance Web Interface, under Miscellaneous, select **Download Files**.
3. Select the **Files to download from the machine I'm using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click the **Download** button.

When the transfer is complete, the message

Files have been successfully downloaded to the server

is displayed.

6. If more than four optional language files need to be downloaded, repeat this procedure.

Copies of the optional language files are now in the `/var/home/ftp/pub` directory and will be automatically installed during the upgrade process.

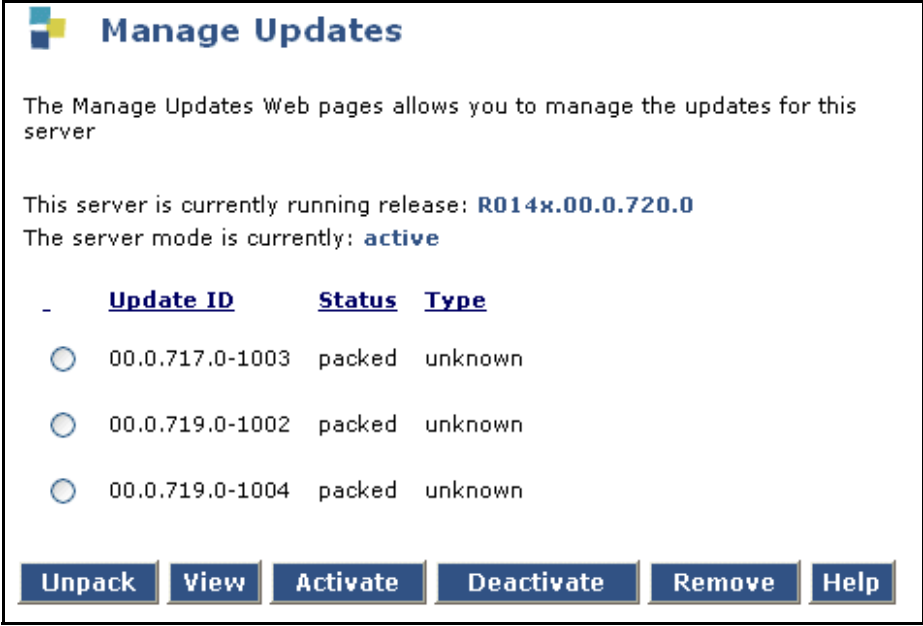
Installing security and Communication Manager service pack updates, if any

To install update files

1. Under Server Upgrades, select **Manage Updates**.

The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allows you to manage the updates for this server

This server is currently running release: **R014x.00.0.720.0**
The server mode is currently: **active**

	<u>Update ID</u>	<u>Status</u>	<u>Type</u>
☐	00.0.717.0-1003	packed	unknown
☐	00.0.719.0-1002	packed	unknown
☐	00.0.719.0-1004	packed	unknown

Unpack View Activate Deactivate Remove Help

2. If an update file you want to activate shows **packed** in the **Status** column, select update ID and click **Unpack**.

The window shows the status of the unpacking.

3. Wait until the system displays the message **Finished unpacking...** and click **Continue**.

The system displays the **Manage Updates** screen.

4. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

5. Click **Yes**.

Wait until the system displays the Continue button.

6. Click **Continue**.

Setting the Time, Date, and Time Zone

To set the Time, Date, and Time Zone:

1. On the Maintenance Web pages, under **Server**, select **Server Date/Time**.

Server Date/Time Window

Server Date/Time

The Server Date/Time Web page lets you reset date and time when the server is used as its own time source.

The current time is: **Wed Aug 20 19:10:00 MDT 2003**

Date (mm/dd/yyyy)

Select time (hh:mm)
Use 24-hour format

Time Zone

2. Set the media server's time close enough to the Network Time Server's (NTS's) time, date, and time zone that synchronization can occur (within about 5 minutes of the NTS time).

CAUTION:

If you are installing an LSP, you must set the time of the LSP to the same time zone as the primary controller even if the LSP is physically located in a different time zone.

Configuring network parameters

Note:

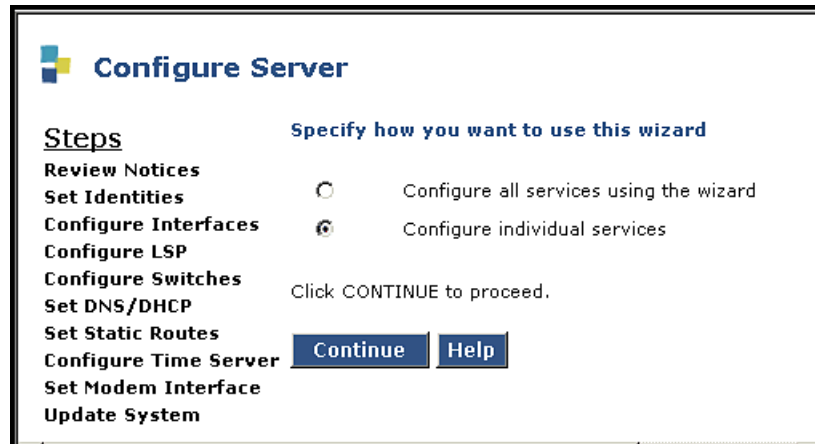
For this procedure, you must have the host name, subnet mask, and IP address of the S8300, and the IP address of the default gateway.

You must configure the network parameters on the S8300 before restoring the backup files. These network parameters are necessary to allow the media server to reach the FTP backup server over the network.

To configure network parameters

1. Under Server Configuration click **Configure Server** to start the configure server process.
2. Click **Continue** through the **Review and Backup Notices** to get to the **Specify how you want to use this wizard** screen.

Specify how you want to use this wizard screen



3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the "Configure Individual IP Services" list on the left.
The **Set Identities** screen appears.
5. Fill in the Host name screen with the name of the server.
6. Click **Continue**.
The **Configure Ethernet Interfaces** screen appears.

Configure Ethernet Interfaces screen (primary controller example)

Configure Server

Configure Interfaces

Ethernet 0: Laptop
 IP address 192.11.13.6
 Subnet mask 255.255.255.252

Ethernet 1: Control Network
 IP address server1 (swainsons-icc) 135.9.127.60
 Gateway 135.9.127.254
 Subnet mask 255.255.255.0
 Speed (Current speed : 100 Megabit full duplex) AUTO SENSE

Integrated Messaging
 IP address server1 (swainsons-icc)

Click **CHANGE** to change values.

Change **Close Window** **Help**

Local intranet

7. Fill in the correct server IP address, Gateway, Subnet mask, and, if IA770 was installed, the Integrated Messaging IP address. The Integrated Messaging IP address is not available with an LSP.

If these fields are already filled in, overwrite them with the correct information. Leave the Integrated Messaging field blank.

Click **Change** to update the system files.

Note:

If an **Action Cancelled** message appears before the success message, refresh the screen and click **Change** again.

8. When the configuration change is complete, the screen displays **Successfully configured ethernet interfaces**. Click **Close Window**.

At this point, the system resets the IP interfaces.

Verifying connectivity

To verify that the Ethernet port is working, ping the FTP server where the backup file(s) are stored.

To verify connectivity

1. On the Maintenance Web Interface, under Diagnostics click **Ping**.
2. Enter the IP address where the Linux-Migration backup file is stored.
3. Click **Execute Ping**.

If the ping is successful, continue with restoring the system files. Otherwise, check the IP address and connectivity to the server.

Disabling RAM disk on the media server

You must disable RAM disk prior to restoring the S8300 configuration data. To disable RAM disk, perform the following steps:

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. At the command line, type `sudo ramdisk -v -f disabled`, and press **Enter**.
The system does not display any information to the screen if there are no errors.
3. At the command line, type `ramdisk -v -s` and press **Enter**.

Rebooting the media server

To reboot the media server, perform the following steps:



CAUTION:

Be sure the DVD/CD-ROM drive is not connected.

1. On the Maintenance Web Interface, under Server select **Shutdown Server**.
2. Select the **Delayed Shutdown** option. Also, be sure the **Restart server after shutdown** checkbox is selected.
3. Click the **Shutdown** button.
Click **OK** to confirm.
4. At the command line, type `ramdisk -v -s` and press **Enter**.
Confirm that the system has disabled RAM disk.

Restoring data backup

Do these tasks:

- if the original release was between **1.2.0** and **1.3.9**, and you performed a Linux Migration backup
- or if the original release was **2.0** or later and you performed a normal data backup

CAUTION:

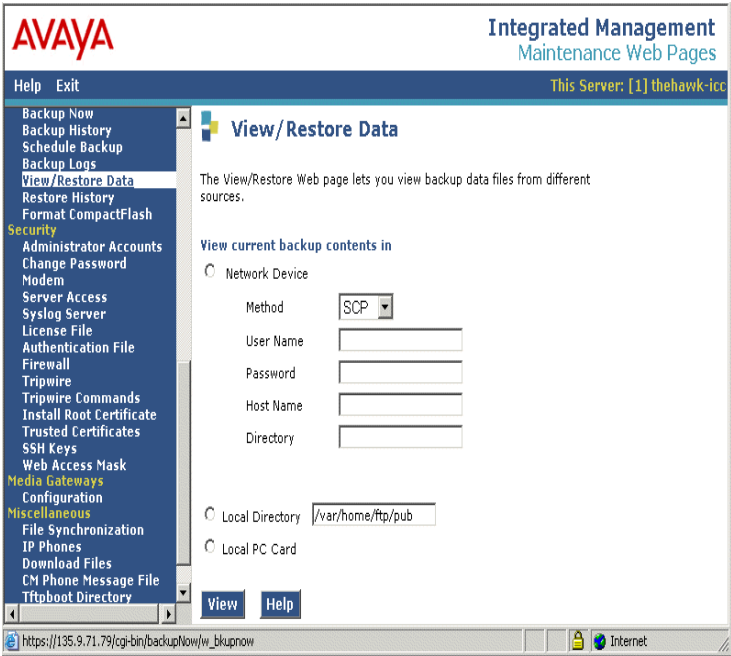
If you used the Linux Migration Backup/Restore backup process, there will be a single backup file with a name starting with "upgrade-2.0." Be sure to restore that backup file, not the backup sets that you may have created with the Data Backup/Restore — Backup Now process. If you restore the wrong files, the system can be damaged and the only recovery path is to remaster the S8300 hard drive again. This recovery procedure can be started using the **remaster** command, which is described in *Maintenance Commands for Avaya Communication Manager, Media Gateways and Servers*, 03-300431. After running the remaster command, reboot the S8300 to start the RP program and proceed with [Remastering the S8300 and installing the upgrade software](#) on page 577.

To restore backup data:

1. On the Maintenance Web Interface, under Data Backup/Restore select **View/Restore Data**.

The system displays the **View/Restore Data** screen.

View/Restore Data screen



AVAYA Integrated Management Maintenance Web Pages

Help Exit This Server: [1] thehawk-icc

View/Restore Data

The View/Restore Web page lets you view backup data files from different sources.

View current backup contents in

☐ Network Device

Method

User Name

Password

Host Name

Directory

☐ Local Directory

☐ Local PC Card

https://135.9.71.79/cgi-bin/backupNow/w_bkupnow

2. Select **FTP**.

Fill in the **User Name**, **Password**, **Host Name (enter host IP Address)**, and **Directory** fields for the location of the backup file on the customer's server.

3. Click **View**.

The system displays the **View/Restore Data Results** screen.

View/Restore Data Results screen

View/Restore Data Results

List of backup images (x.tar.gz) at specific location:

File Name

- ☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_092458_20031121.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_094952_20040420.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_125559_20040502.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_162851_20040428.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_092507_20031121.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_095003_20040420.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_125611_20040502.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_162903_20040428.tar.gz
- ☒ /usr/add-on/systest/translations/doc-icc1/upgrade-2.0_doc-icc1_105127_20030909.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/upgrade-2.0_doc-icc1_160417_20030908.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_092435_20031121.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_094933_20040420.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_125534_20040502.tar.gz
- ☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_162828_20040428.tar.gz

Pass Phrase:

☐ Force restore if server name mismatch.

☐ Force restore if backup version mismatch.

Restore **Preview** **Help**

4. Select the backup file to restore.

If you started with a software release between 1.2.0 and 1.3.x and you used the Linux-Migration Backup procedure, the backup file name will start with "upgrade-2.0."

If you started with a 2.0.x software release and you used the Backup Now procedure, there are three backup files with names starting with "os," "xln," and "security." Restore only the "os" file first.

Note that the time and date are embedded in the file name. Select the backup sets with the current time and date stamp.

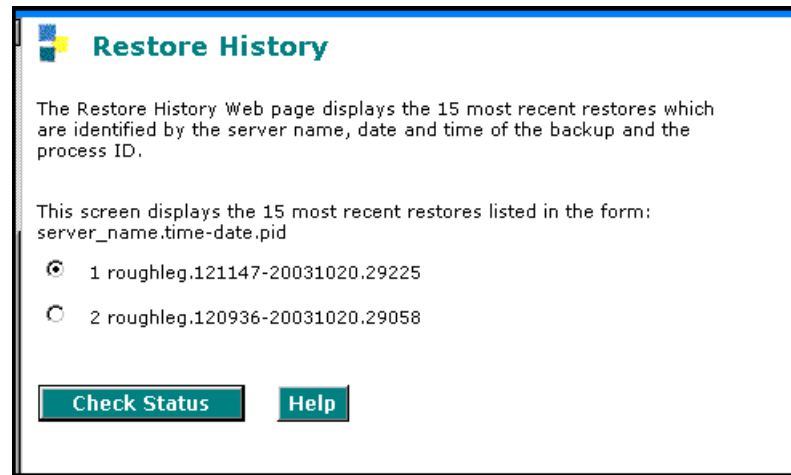
5. Select both **Force** options, and click **Restore**.

6. To monitor the restore progress:

a. Select **Restore History**

The **Restore History** screen displays.

Restore History screen



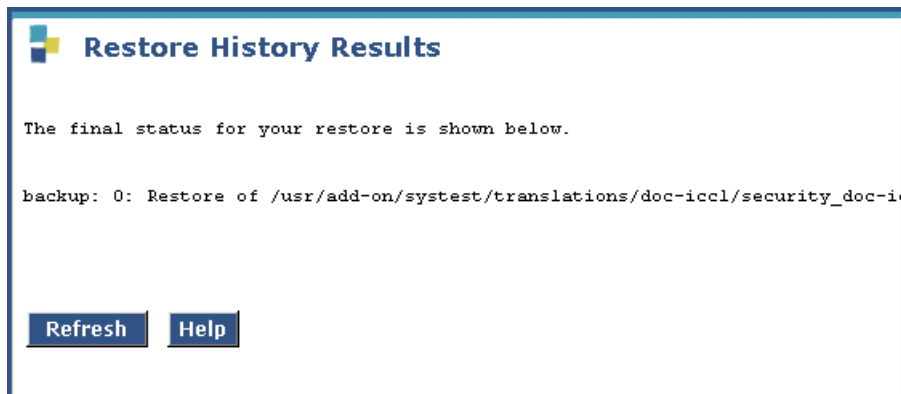
- b. Select the backup set being restored and click **Check Status**.

The **Restore History Results** screen displays.

- c. Click **Refresh** periodically until the message,

The final status for your restore is shown below appears.

Restore History Results screen



7. If you started from Release 2.0, repeat the restore procedure for the remaining backup sets in the following order:

Note:

If you restored a full backup, you do not need to restore the security and translations data backups.

- Security data in the file whose name begins with "security."
- (For a primary controller only, not an LSP) Translations data in the file whose name begins with "xln."

- (For a primary controller only, not an LSP) If IA770 was installed, INTUITY AUDIX data in the file whose name begins with "audix-tr-name-msg."
- (For a primary controller only, not an LSP) If IA770 was installed, INTUITY AUDIX data in the file whose name begins with "audix-ann".

Checking for the IA770 IP address

1. Under Server Configuration click **Configure Server** to start the configure server process.
2. Click **Continue** through the **Review and Backup Notices** to get to the **Specify how you want to use this wizard** screen.
3. Click **Configure Interfaces** from the "Configure Individual IP Services" list on the left.

The **Configure Interfaces** screen displays.

Configure Interfaces screen (primary controller example)

Configure Server

Configure Interfaces

Ethernet 0: Laptop

IP address 192.11.13.6

Subnet mask 255.255.255.252

Ethernet 1: Control Network

IP address server1 (swainsons-icc) 135.9.127.60

Gateway 135.9.127.254

Subnet mask 255.255.255.0

Speed (Current speed : 100 Megabit full duplex) AUTO SENSE

Integrated Messaging

IP address server1 (swainsons-icc)

Click CHANGE to change values.

Change Close Window Help

4. Check that the Integrated Messaging IP address is available.

5. If the IP address is available, click Close Window.
6. If the IP address is not available, enter the IP address and click Change.

Note:

If an **Action Cancelled** message appears before the success message, refresh the screen and click **Change** again.

When the configuration change is complete, the screen displays **Successfully configured ethernet interfaces**. Click **Close Window**.

At this point, the system resets the IP interfaces.

Enabling RAM disk on the media server

To enable RAM disk, perform the following steps:

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. At the command line, type `sudo ramdisk -v -f enabled`, and press **Enter**.
3. At the command line, type `ramdisk -v -s` and press **Enter**.

Rebooting the media server

To reboot the media server, perform the following steps:

1. On the Maintenance Web Interface, under Server select **Shutdown Server**.
2. Select the **Delayed Shutdown** option. Also, be sure the **Restart server after shutdown** checkbox is selected.
3. Click the **Shutdown** button.
Click **OK** to confirm.
4. At the command line, type `ramdisk -v -s` and press **Enter**.
Confirm that the system has enabled RAM disk.

Note:

It is good practice to close the browser after the reboot and log back in.

Installing updated license and authentication files



CAUTION:

A super-user login, dadmin or another customer superuser login, must exist *before* you install an authentication file. If the authentication file does not install, you might need to create a super-user login, then install the new authentication file. See [Checking a 4.0 release for a super-user login](#) on page 595.

To install the license and authentication files:

1. On the Maintenance Web Interface menu under Security, select **License File**.

The **License File** screen displays.

License File Screen

License File

The License File Web page allows installation of Avaya license files.

CommunicationsMgr License Mode: Normal
Network used for License: Carrier MGP
License Serial Number is 01DR12310260 on carrier MGP

☐ Undo last install
☒ Install the license file I previously downloaded
☐ Install the license file specified below

File Path
URL
Proxy Server e.g proxy.domain:3152

2. Select **Install the license file I previously downloaded** and click **Submit**.

The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.
4. The **Authentication File** screen displays.

Authentication File screen

Authentication File

The Authentication File Web page allows installation of Avaya authentication files.

☒ Install the Authentication file I previously downloaded
☐ Install the Authentication file I specified below

File Path

URL

Proxy Server (e.g. proxy.domain:3152)

5. Select **Install the Authentication file I previously downloaded** and click **Install**.

The system tells you the authentication file is installed successfully.

Note:

If the authentication file failed to install, see [Checking a 4.0 release for a super-user login](#) on page 595. The system may not have had a super-user login.

Checking a 4.0 release for a super-user login

To ensure that a super-user login exists in Communication Manager in Release 4.0 or higher:

1. Log in with **ssh**.
2. At the Linux command line, type `cat /etc/passwd | grep 555`.

The following list of super-user logins appears.

```
init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1001:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash
```

3. Look for any logins other than the init, inads, and craft logins. If no additional super-user logins exist, you must create one. See [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 596.

Creating a super-user login, if necessary, for R4.0 or higher

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages. Use the following steps only if you are starting from Release 4.0 software or later:

Note:

A craft level login can create a super-user login in Release 4.0 or later.

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

To create a login:

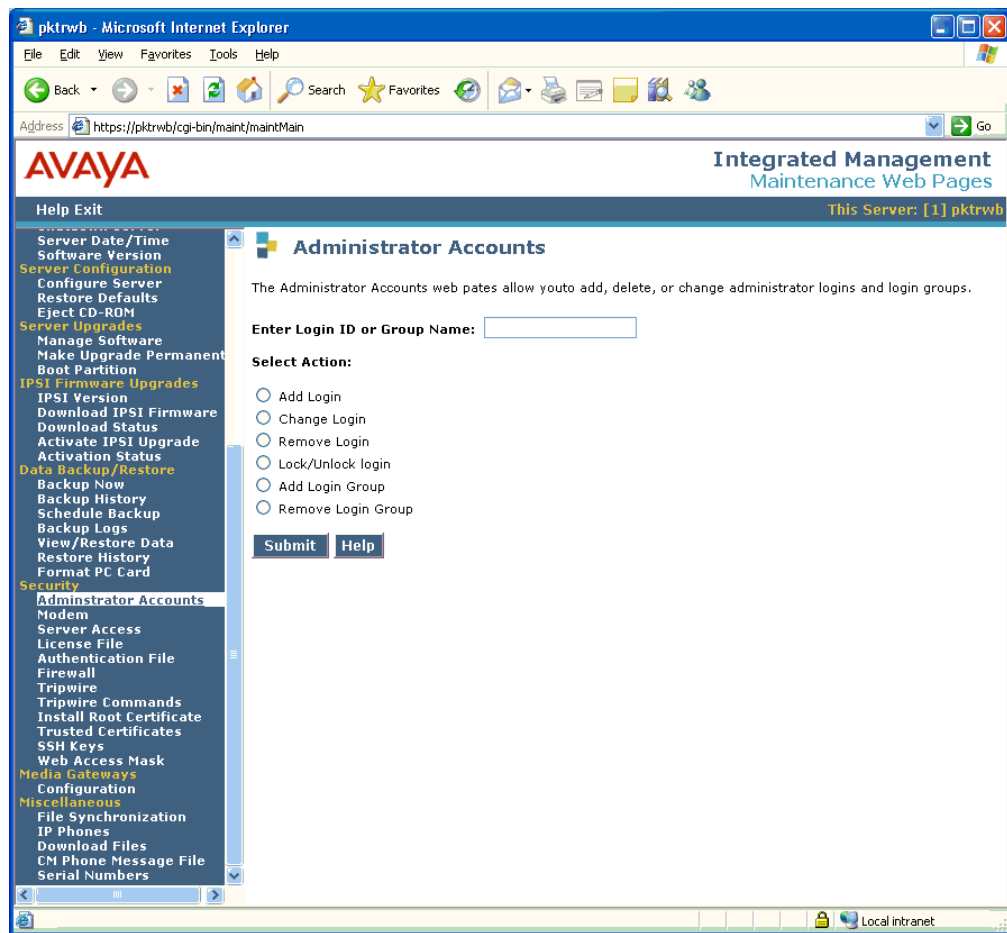
1. Ask a customer representative for a login name and password that the customer would like for the superuser login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Note:

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

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



3. Type the login name in the **Enter Login ID or Group Name** field.

4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The top header includes the Avaya logo and the title 'Integrated Management Maintenance Web Pages'. Below the header, there is a navigation menu on the left with categories like 'Server Upgrades', 'IPSI Firmware Upgrades', 'Data Backup/Restore', and 'Security'. The main content area displays the 'Add Login' form. The form includes fields for 'Login ID' (set to 'randy'), 'login group' (set to 'susers'), 'additional groups' (set to 'prof18'), 'allow Linux shell access' (checkbox), 'lock this account' (checkbox), 'date (YYYY-MM-DD) on which account is disabled (blank to ignore)', 'select type of authentication' (radio buttons for 'password' and 'ASG'), 'enter key or password', 're-enter key or password', 'force password/key change on first login' (radio buttons for 'yes' and 'no'), 'maximum Number of days a password may be used (PASS_MAX_DAYS):', 'minimum number of days allowed between password changes (PASS_MIN_DAYS):', 'minimum acceptable password length (PASS_MIN_LEN):', 'number of days warning given before a password expires (PASS_WARN_AGE):', and 'days after password expires to lock account (0=immediate)'. The 'Add' and 'Help' buttons are at the bottom of the form.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

10. Complete the following fields:

- enter a challenge key or password
- re-enter challenge key or password
- force password/key change on first login

Note:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

- a. Log in with `telnet` or `ssh`.
- b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If upgrading an LSP, synchronize translations from the primary controller

If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

1. Log in with `telnet` or `ssh`.
2. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`
3. Type `start -ca`

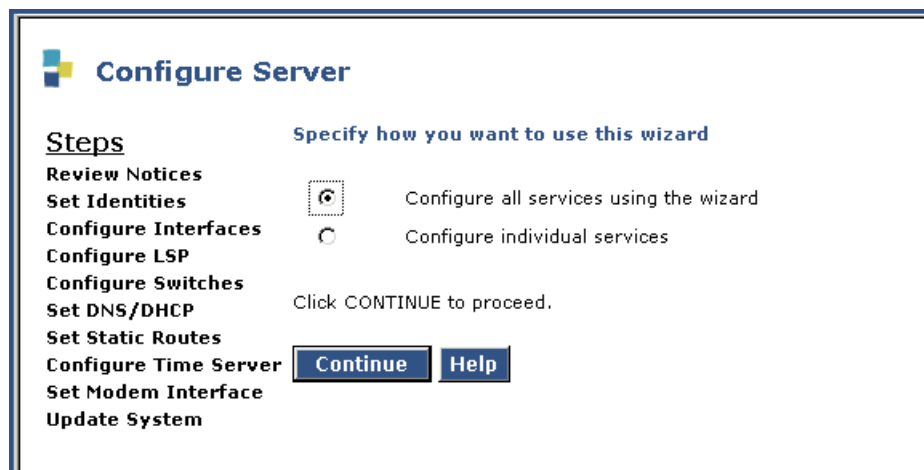
Verifying media server configuration (Release 1.2 or later)

At this point, you should not have to enter any configuration information. In the following procedure, click **Continue** to open each configuration screen and verify the that configuration information is correct.

To verify media server configuration

1. Under Server Configuration click **Configure Server** to start the configure server process.
Click **Continue** until you reach the screen titled **Specify how you want to use this wizard**.

Specify how you want to use this wizard screen



2. Select **Configure all services using the wizard**.
3. Click **Continue** through all the screens.

Check for new screens and new fields on existing screens as mentioned in the planning forms.

Note:

You must click **Continue** through all the screens whether there are changes or not. You **do not** need to enter **Static Network Route** information.

4. Click **Continue** on the **Update System** screen.

The **Updating System Files** screen displays each configuration task as it completes. When done, the screen displays the line **All configuration information was entered**.

5. Click **Close Window**.

6. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

7. Type `/opt/ws/drestart 1 4` to initialize the application process using the restored configuration data.

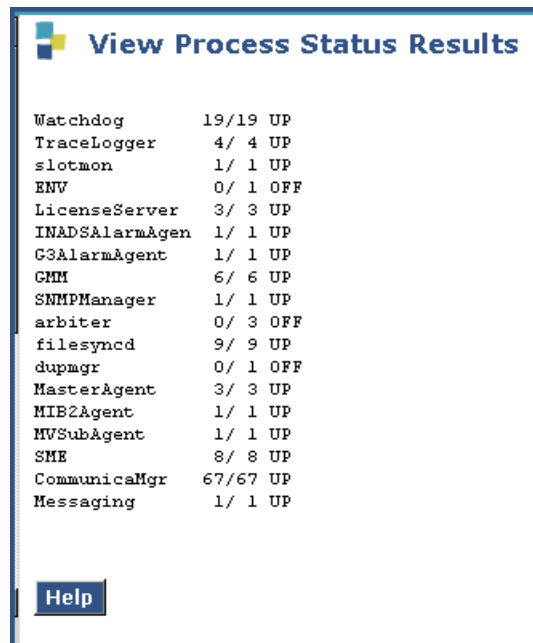
You should see the response, Killed.

If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started

If you installed IA770 INTUITY AUDIX Messaging, the messaging application should start after you install the license. To verify that messaging has started, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.
the **View Process Status Results** screen displays.

View Process Status screen



View Process Status Results		
Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

Help

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

If you need to start messaging, you can use either the Maintenance Web pages or the Linux command line. For the Maintenance Web pages, see [Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary](#) on page 602. For the Linux command line method, see [Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary](#) on page 602.

Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary

1. From the Maintenance Web Page, select **Messaging Administration** from the **Miscellaneous** menu.

The Messaging Administration Web page is displayed in a new Web browser window.

2. From the Messaging Administration Web page, select **Utilities**.

The Utilities Web page is displayed.

3. Select **Start Messaging Software**.

The Start Messaging Software Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

2. Type **start -s Audix**

3. Ensure that all Communication Manager processes come up.

To monitor the startup of IA770:

- a. Type **watch /VM/bin/ss**

The display will periodically refresh automatically. When you see the following display, the IA770 startup is complete.

- b. Press **Ctrl+C** to break out of the **watch** command.

If IA 770 fails to start after an upgrade

If you have upgraded your Communication Manager and IA 770 INTUITY AUDIX software, you must have a new license that is associated with the latest release. IA 770 will not use the license for a previous version.

If you upgraded IA 770 without a new license file, it will fail to start during the Communication Manager startup sequence.

If this occurs, you must do the following steps:

1. Obtain an IA 770 Replace variable w/ release number license file.
2. Install the license file.
3. From a command prompt, start the IA 770 process with the following command:

```
start -s Audix
```

Saving translations

Note:

If the S8300 you are upgrading is an **LSP**, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session. and log in as *craft* (or *dadmin*).
2. If the S8300 you are upgrading is a primary controller, at the SAT prompt, type **save translation** and press **Enter**.
3. If the S8300 you are upgrading is an LSP, then on the primary controller, type **save translation lsp** and press **Enter**. This command distribute saved translations out to the LSPs.

When the save is finished, the system displays the message,

```
Command successfully completed.
```

The system automatically performs a reset system 4. If you are upgrading an LSP, you are logged out.

Upgrade the firmware on the G700 Media Gateway

Conduct the following manual procedures to update the firmware running on the G700 Media Gateway processors and media modules. Alternate methods to upgrade the G700 Media Gateway include using the Avaya Installation Wizard, the Upgrade Tool, or Software Update Manager.

Verifying the contents of the *tftpboot* directory

Before proceeding with the G700 firmware installation, you should check the */tftpboot* directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the */tftpboot* directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.
2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the */var/home/ftp/pub* directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the *pub* directory.

3. Copy the firmware files from the *pub* directory to the */tftpboot* directory, using the S8300 Media Server command line interface.

To copy firmware files to the */tftpboot* directory of an S8300 Media Server, do the following:

- a. Use SSH, Avaya Site Administration, or another tool to access the S8300 Media Server command line.
- b. Log in as *craft*.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to */var/home/ftp/pub*.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the */tftpboot* directory. To copy multiple firmware files (most firmware files have an *.fdl* suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the */tftpboot* directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to */tftpboot*.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

Conduct the following procedure to compare software versions running on the G700 processors and media modules with the versions in your planning documents. If the versions do not match, you need to install the new firmware for those components.

To determine if new firmware for the P330 stack processor is necessary

1. At either the **P330-1(super)#** or **P330-1(configure)#** prompt, type **dir**.

The system displays the directory list of software for the P330 stack processor.

Directory list for P300 stack processor

M#	file	ver num	file type	file location	file description
--	----	-----	-----	-----	-----
1	module-config	N/A	Running Conf	Ram	Module Configuration
1	stack-config	N/A	Running Conf	Ram	Stack Configuration
1	EW_Archive	4.0.4	SW Web Image	NV-Ram	WEB Download
1	Booter_Image	3.2.5	SW BootImage	NV-Ram	Booter Image

2. Check the version number (ver num) of the EW_Archive file to see if it matches the Release Letter.

If not, you must upgrade the P330 stack processor.

3. Type **show image version**

The system displays the list of software.

Show image version List for P330 stack processor

Mod	Module-Type	Bank	Version
-----	-----	----	-----
3	Avaya G700 media gateway	A	0.0.0
3	Avaya G700 media gateway	B	4.0.17

4. Check the version number of the stack software image file in Band B to see if it matches the your planning document.

If not, you must upgrade the P330 stack processor.

To determine if new firmware is required for the MGP, VoIP module, and installed media modules

1. Type **session mgp**
2. At the **MG-001-1(super)#** prompt, type **show mg list_config**

The system displays the list of software.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (B)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

3. Refer to the list to check the FW vintage number of the G700.

In the TYPE column, find G700, then check the matching field in the FW VINTAGE column to see if it matches the vintage number in your planning forms. If not, you must install new firmware on the G700 media gateway. Also check if the release number in the FW VINTAGE column contains (A) or (B) to designate the software bank. If the list shows B, you will upgrade A. If the list shows A, you will upgrade B.

4. Refer to the VOIP FW column and row for slot V0 (same row occupied by the G700 information) to see if the number matches the VoIP firmware identified in your planning forms.

If not, you must also upgrade the G700 media gateway motherboard VoIP module.

Note:

The VoIP processor on the motherboard is upgraded using the same firmware image file as the VoIP media modules; for example, the file mm760v8.fdl is vintage #8.

5. Check the FW VINTAGE column for vintages of each of the installed media modules: MM710, MM711, MM712, MM720, and/or MM760 to see if they match the FW vintages in the planning forms.

If not, you must upgrade them, as well.

Installing new firmware on the P330 Stack Processor

To install P330 stack processor firmware

1. From your S8300 telnet session, telnet back to the P330 stack processor:

Type `telnet <xxx.xxx.xxx.xxx>`

where `<xxx.xxx.xxx.xxx>` is the IP address of the P330 stack master processor on the customer's LAN.

- At the **P330-1(configure)#** prompt, type

```
copy tftp SW_image <file> EW_archive <ew_file>
<tftp_server_address> <Module#>
```

where **<file>** is the full-path name for the image file with format and vintage number similar to viisa3_8_2.exe,

<ew_file> is the full-path name for the embedded web application file with format similar to p330Tweb.3.8.6.exe,

<tftp_server_ip_address> is the IP address of the TFTP server, and

<Module#> is the number, 1 through 10, of the media gateway in the stack. If there is only one G700 media gateway, the number is 1.

- Verify that the download was successful when the prompt returns:
 - type **show image version <module #>** and check the version number in the Version column for Bank B.
 - type **dir <module #>** and check the version number in the ver num column for the EW_Archive file.
- Type **reset <module #>**.

Installing new firmware on the G700 Media Gateway Processor

To install MGP firmware

- At the **P330-1(configure)#** prompt, type **session mgp** to reach the G700 media gateway processor.
- Type **configure** at the **MG-???-1(super)#** prompt to enter configuration mode, which will change the prompt to **MG-???-1(configure)#**.
- At the **MG-???-1(configure)#** prompt, type **show mgp bootimage** to determine which disk partition (bank) is in the **Active Now** column.

You will update the bank that is *not* listed as Active Now. The system displays the following screen:

Example: Show mgp bootimage

<u>FLASH MEMORY</u>	<u>IMAGE VERSION</u>
Bank A	109
Bank B	210
<u>ACTIVE NOW</u>	<u>ACTIVE AFTER REBOOT</u>
Bank B	Bank B

4. At the **MG-???-1(configure)#** prompt, type

```
copy tftp mgp-image <bank> <filename> <tftp_server_ip_address>
```

to transfer the mgp image from the tftp server to the G700,

where

<bank> is the bank that is *not* Active Now (Bank A in the example).

<filename> is the full path name of the mgp firmware image file, which begins with mgp and will be similar to the name mgp_8_0.bin.

<tftp_server_ip_address> is the IP address of the S8300.

For example:

```
copy tftp mgp-image a mgp_8_0.bin 195.123.49.54
```

The screen shows the progress.

5. Type **set mgp bootimage <bank>**

where **<bank>** is the same letter you entered in the previous step.

6. At the **MG-???-1(configure)#** prompt, type **reset mgp**.

A system prompt asks you to confirm the reset.

7. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

8. When the **P330-1(super)#** prompt appears, type **session mgp**.

9. At the **MGP-???-1(super)#** prompt, type **configure**.

10. Verify that the download was successful when the prompt returns.

Type **show mg list_config**.

The system displays the list of software.

Example: Show mg list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	230 (A)	67
V1	ICC	S8300	A	72	00	N/A
V2	DCP	MM712	A	2	58	N/A
V3	ANA	MM711	A	2	57	N/A
V4	DS1	MM710	A	1	58	N/A

Installing new firmware on the media modules

For upgrades of active media modules, you need to take the media modules out of service before initiating the upgrade process. To do this, go to a SAT session on the primary controller and issue a `busyout` command.

Note:

Skip this busyout procedure if the media modules are not in service; for example during an initial installation.

To busyout board (for active media modules)

1. Go to a SAT session on the primary controller and enter the command,
`busyout board vx`
where `x` is the slot number of the media module to be upgraded.
2. Verify the response,
`Command Successfully Completed`
3. Repeat for each media module to be upgraded.

To install media module firmware

1. Be sure that you have checked for the current vintage of the VoIP Module for the v0 slot (on the G700 motherboard).
This VoIP module does not occupy a physical position like other media modules.
2. At the **P330-1(configure)#** prompt, type `session mgp`.
3. At the **MG-001-1(super)#** prompt, type `configure` to change to the configuration mode.
4. Type `copy tftp mm-image v<slot #> <filename mm>`
`<tftp_server_ip_address>`
where
`<slot #>` is the slot of the specific media module,

`<filename mm>` the full-path name of the media module firmware file in a format such as `mm712v58.fdl`, and

`<tftp_server_ip_address>` is the ip address of the S8300.
Two or three minutes will be required for most upgrades. The VoIP media module upgrade takes approximately 5 minutes. Screen messages indicate when the transfer is complete.
5. After you have upgraded all the media modules, verify that the new versions are present.
At the **MG-???-1(configure)#** prompt, type `show mg list_config`
The list of software appears.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
V0	G700	DAF1	A	00	21.25.0 (A)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

- In the **TYPE** column, find the particular media module (v1 through v4), then check the matching field in the **FW VINTAGE** column to see if it matches the planning documentation.

Note:

Slot V1 can contain either a media module or the S8300, which will show as
TYPE ICC.

- Check the **VOIP FW** column and row for slot v0 to see if the number matches the VoIP firmware identified in the planning documentation.
- Type **reset <module #>**
where **<module #>** is the number of the G700 in the stack.
- When the reset is finished, type **show mm** to verify the upgrade.

To release board (if media module was busied out)

- When the upgrade procedure is complete, go to the SAT session and release the board
Type **release board vx**
where **x** is the slot number of the upgraded media module.
- Verify the response,
Command Successfully Completed

Note:

If you see the response, Board Not Inserted, this means that the media module is still rebooting. Wait one minute and repeat the **release board** command.

- Repeat the **release board** command for each media module that was busied out.

Ensuring the MGP default gateway IP address is set

Communication Manager release 4.0 requires that the built-in VoIP module of the G700 Media Gateway has a default gateway IP address. To ensure that this IP address is set, perform the following steps:

1. At the **MG-???-1(configure)#** prompt, type **show ip route mgp**.

The list of mgp routes appears.

```
MG-001-1(super)# show ip route mgp
```

DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	135.9.80.254	motfec0	(3/0/165)
135.9.80.0	255.255.255.0	135.9.80.88	motfec0	(101/0/0)

```
MG-001-1(super)#
```

2. Check that a Gateway IP address exists for Destination 0.0.0.0.
3. If a Gateway IP address does not exist, type, at the **MG-???-1(configure)#** prompt, **set ip route 0.0.0.0 0.0.0.0 <IP_address>**, where **<IP_address>** is the default gateway IP address.

After you reboot the media gateway, the IP address is active and available.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 stack processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.

4. To set the **rapid spanning tree** version, type `set spantree version rapid-spanning-tree` and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command `set port spantree cost auto`.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type `set port edge admin state module/port edgeport`.

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* (available at <http://www.avaya.com/support>).

Installing new firmware on other G700 media gateways

Installing G700 firmware in a stack configuration

If the customer has multiple G700 media gateways connected in an IP stack, you can stay connected to the master G700/P330 and "session" over from the master P330 Stack Processor to the next G700 in the stack. If you are dialed in remotely, you should have automatically dialed in to the stack master. For a local installation, you should have plugged your laptop into the stack master P330, which you can identify by the LED panel on the upper left of each G700 or P330/C360 device in the stack.

The LEDs signal as follows:

- On the G700 Media Gateway: a lit **MSTR** LED indicates that this unit is the stack master.
- On the P330 or C360 device: a lit **SYS** LED indicates that this unit is the stack master.

The G700 and P330/C360 at the bottom of the stack is module number 1, the next module up is number 2, and so on. However, the stack master can be any module in the stack, depending on the actual model, the vintage firmware it runs, and whether the S8300 is inserted into it.

Note:

You do not need to configure the other P330 or C360 processors in the stack. These will use the IP address and IP route of the master stack processor. However, you will need to check firmware on all devices of the other G700s in the stack, including the media gateways themselves, and update the firmware as required.

You may also use the "session stack" command to access other standalone P330 or C360 processors in the stack (those that are not part of a G700 unit).

To "session" over to another G700/P330/C360 in a stack

1. At the **MG-001-1(configure)#** prompt, type `session stack`
The **P330-1(configure)#** prompt appears.
2. At the **P330-1(configure)#** prompt, type `session <mod_num> mgp`
where `<mod_num>` is the next P330 or C360 processor in the stack.
If you are currently logged in to the master stack processor, `<mod_num>` would be `2`, for the second G700/P330/C360 processor in the stack.
3. For other G700s in the stack, repeat the steps described previously to install firmware for the stack processor, MGP, and media modules.

Installing G700 firmware in a remote, no stack configuration

If additional G700 media gateways are supported in the configuration, but they are not attached as a stack, then you must configure each G700, with all of its devices, including the P330 processors. Additionally, you must check firmware and update the firmware as required.

Post-upgrade tasks

Complete the following tasks after you have finished the upgrade:

Stopping IA770 INTUITY AUDIX Messaging, if installed

After the upgrade is complete, perform the following post-upgrade tasks.

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing IA770 service pack (or RFU) files, if any

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at <http://support.avaya.com>.

1. Select **Messaging Administration** from the main menu.
2. Select **Utilities** from the Messaging Administration menu.
3. Select **Software Management** from the Utilities menu.
4. Select **Advanced Software Installation** from the Software Management menu.
5. Select **Continue this operation without current system backup**.
6. Select the IA770 update package and click **Install Selected Packages**.

Note:

The system automatically prompts you to restart INTUITY AUDIX when the service pack has been installed. Therefore, if you restart AUDIX at this time, you do *not* need to perform the following procedure, [Starting IA770 INTUITY AUDIX Messaging, if installed](#).

Starting IA770 INTUITY AUDIX Messaging, if installed



CAUTION:

You do *not* need to perform this task if you restarted AUDIX as a part of the installation of the IA770 service pack.

After the IA770 INTUITY AUDIX Messaging application has been updated, you must restart it using the following steps:

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Start Messaging Software**.

The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

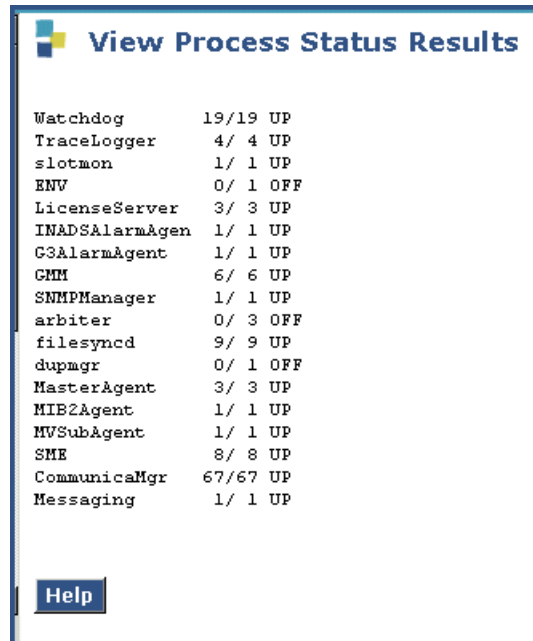
4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Verifying start up of IA770 INTUITY AUDIX Messaging, if installed

To verify operation of IA770 INTUITY AUDIX Messaging, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.
the **View Process Status Results** screen displays.

View Process Status screen



View Process Status Results		
Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

Help

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an IA770 sanity test:
 - a. At the Linux command line, type `/vs/bin/display`
 - b. All states should be `Inserv` with an associated phone number.
 - c. Retrieve the test message saved before the upgrade.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.
3. Type **save translation** and press **Enter**.

When the save is finished, the system displays the message,

`Command successfully completed.`

If using IA770, administering switch integration for H.323

The IA770 INTUITY AUDIX Messaging application uses H.323 signaling instead of the CWY1 board for integration with Communication Manager. The tasks for administering the H.323 integration are explained in *Administering Media Servers to work with IA770*.

Administering IA770 (Release 1.3 or earlier)

Because IA770 INTUITY AUDIX Messaging messages, names, and administration are not restored for releases prior to Release 2.0, the customer must readminister IA770 INTUITY AUDIX Messaging, including recording names and custom announcements. See the *IA770 INTUITY AUDIX Messaging Application 4.0 Documentation Library* CD-ROM.

Testing to verify system functionality

Test the system for functionality, if you are upgrading an S8300 primary controller;

1. Verify the following:
 - Telephones have dial tone
 - You can call from one telephone to another telephone on the system
 - You can make an external trunk call.
 - The media gateways have registered. Use the SAT command **list media-gateway**.

Complete the upgrade process (S8300 is the primary controller)

In an SSH session to the S8300 (primary controller), access the SAT command line interface to complete the following procedures.

To check media modules

1. Type `list configuration all` and press **Enter**.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that Communication Manager is working.

To enable scheduled maintenance

1. Type `change system-parameters maintenance` and press **Enter**.
2. Ensure that the **Start Time** and **Stop Time** fields' administration is the same as before the upgrade.

To busy out trunks

1. Busy out trunks that were busied out before the upgrade (see [Completing pre-upgrade tasks — if the S8300 is the primary controller](#) on page 557).

To check for translation corruption

1. Type `newterm` and press **Enter**.

If you do not get a login prompt and see the following message:

Warning: Translation corruption detected

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To resolve alarms

1. On the Maintenance Web Interface, under Alarms click **Current Alarms** to examine the alarm log.
2. If any alarms are listed, click **Clear All**.
3. Resolve new alarms since the upgrade through Communication Manager using the appropriate maintenance reference.

To re-enable alarm origination

1. Telnet to the S8300 and log on.
2. At the command prompt, type `almenable -d b -s y`
where
`-d b` sets the dialout option to *both* (numbers)
`-s y` enables SNMP alarm origination
3. Type `almenable` (without any options) to verify the alarm origination status.

To back up the system

Using the Maintenance Web Interface, back up the system as you did before the upgrade selecting **Save Translations** and all backup sets.

To restart LSPs (if any)

To restart Communication Manager on LSPs (if any) after the upgrade:

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. At the command prompt, type `start -ac` and press **Enter**.

This completes the upgrade process for a G700 with an S8300.

Chapter 11: Manual upgrade of an existing S8300B or S8300C and G700 to R4.0

This chapter covers the procedures to upgrade the software on an installed Avaya S8300B or S8300C Media Server from a 2.x or 3.x release to 4.x. The procedures to upgrade the G700 firmware use CLI commands instead of the Upgrade Tool. This chapter also covers the procedures to upgrade the firmware on an installed Avaya G700 Media Gateway.



Important:

This chapter assumes that the currently installed S8300 is version B or C. The S8300B is required to run Communication Manager release 2.0 or greater. The S8300C is required to run Communication Manager release 4.0. If the currently installed S8300 is version A, follow the upgrade procedures in [Chapter 10: Manual upgrade of an S8300A and G700 to R4.0](#)

Considerations for upgrading the S8300B or S8300C as a primary controller or as an LSP

The S8300 can be configured as either the primary controller or as a local survivable processor (LSP). When the S8300 is an LSP, the primary controller, running Avaya Communication Manager, can be either another S8300 or an S8400, S8500, or S8700-series Media Server.

 CAUTION:

When you are upgrading the media server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the media server to a release that is not supported as an upgrade path, you might corrupt the translations.

Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.

To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access <http://support.avaya.com>. Select **Downloads > Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates > Latest Communication Manager Software & Firmware Compatibility Matrix**.

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

- The version of Communication Manager running on the LSP must be exactly the same as, or a later version that is compatible to, the version running on the primary controller.
- If upgrading both the primary controller and the LSP to the same release, you must upgrade the LSP first. Next, you upgrade the G700 Media Gateways, including the G700 Media Gateway that houses the primary controller, if the primary controller is an S8300. Then, with Communication Manager turned off on the LSP, you upgrade the primary controller.

Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323

 CAUTION:

Communication Manager Release 4.0 does not support the CWY1 integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current IA770 integration administration before the upgrade and then administer the integration to H.323 after the upgrade.

For instructions on converting the integration to H.323, including the removal of existing administration, see *Administering Media Servers to work with IA770*, 07-600788.



CAUTION:

Be sure to test the new integration before completing the upgrade.

The need to restore IP Phone files

During an upgrade, any data in the /tftpboot directory is overwritten with new software and firmware. If the system was using the http or tftp capability for 4600-series phone firmware downloads and configuration updates, the firmware and 4600-series phone configuration file are overwritten.

You must retrieve the 46xx firmware (the 46xx .tar file, for example **46xxH323_cm2_2_wi1_15_ipt2_2_111405.tar**) from the Avaya Downloads Web site and download the 46xx firmware file to the server after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the /tftpboot directory *after* the upgrade. See the following:

- [Saving a copy of the 4600-series phone configuration file, if any](#) on page 641
- [Copying IP Phone firmware to the media server, if necessary](#) on page 667
- [Restoring the 4600-series phone configuration file, if any](#) on page 668

Tasks to upgrade the S8300B or S8300C to release 4.0 and upgrade the G700 firmware

The major tasks to upgrade the S8300B or S8300C to release 4.x and upgrade the G700 firmware are:

Before going to the customer site

- [Getting information that the project manager provides](#) on page 623
- [Getting the serial number of the G700, if necessary](#) on page 624
- [Checking the number of allocated ports](#) on page 624
- [Checking for and FTP/SCP/SFTP Server or Compact Flash for Backing up Data](#) on page 624
- [Obtaining S8300 software and G700 firmware](#) on page 625
- [Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary](#) on page 627
- [Completing the RFA process \(obtaining license and password file\)](#) on page 629

On-site Preparation for the Upgrade

- [Accessing the S8300](#) on page 637
- [Removing the administration for the IA770 integration if CWY1 board is used](#) on page 638
- [Completing pre-upgrade tasks — if the target S8300 is the primary controller](#) on page 638
- [Saving a copy of the 4600-series phone configuration file, if any](#) on page 641
- [Getting IA770 \(AUDIX\) Data and Stopping IA770 \(if IA770 is being used\)](#) on page 642
- [Ensuring a super-user login exists](#) on page 631
- [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#) on page 633
- [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 634
- [Backing up S8300 recovery system files](#) on page 647
- [Copying and installing the service pack files to the media server \(starting from R2.x only\)](#) on page 649
- [Copying the software and firmware files to the server](#) on page 652

Upgrade the S8300

- [Installing new software](#) on page 657
- [Installing updated authentication files](#) on page 660
- [Installing security and Communication Manager service pack updates, if any](#) on page 662
- [If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started](#) on page 664
- [Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary](#) on page 665
- [Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary](#) on page 665
- [Test to verify system functionality](#) on page 666
- [Test to verify system functionality](#) on page 666
- [Making the upgrade permanent](#) on page 666
- [Saving translations](#) on page 666
- [Copying IP Phone firmware to the media server, if necessary](#) on page 667
- [Restoring the 4600-series phone configuration file, if any](#) on page 668

Upgrade the G700 Firmware

- [Verifying the contents of the tftpboot directory](#) on page 668
- [Determining which firmware to install on the G700](#) on page 669
- [Installing new firmware on the P330 stack processor](#) on page 671

- [Installing new firmware on the G700 Media Gateway Processor](#) on page 672
- [Installing new firmware on the media modules](#) on page 673
- [Installing new firmware on other G700 media gateways](#) on page 677

Post-upgrade tasks

- [Installing IA770 service pack \(or RFU\) files, if any](#) on page 678
- [To check media modules](#) on page 682
- [To enable scheduled maintenance](#) on page 682
- [To busy out trunks](#) on page 682
- [To check for translation corruption](#) on page 682
- [To resolve alarms](#) on page 682
- [To re-enable alarm origination](#) on page 683
- [Backing up the system](#) on page 683

Before going to the customer site

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

Obtaining a USB DVD/CD-ROM drive

Upgrading Communication Manager on an S8300 to release 4.0 requires remastering the S8300B/C hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD/CD-ROM drive at the site.

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Getting the serial number of the G700, if necessary

To get the serial number of the G700 Media Gateway, ask the customer's administrator to:

1. Log in to the S8300 Maintenance web pages.
2. Select **View License Status** or **License File** from the main menu to display the serial number.

Note:

The serial number should also be on a sticker on the back of the G700 chassis, but this number is occasionally incorrect.

Checking the number of allocated ports

Release 4.0 of Communication Manager supports a maximum of 900 ports if the S8300 is a primary controller. If the existing system has more than 900 ports allocated, then there may be a problem with the upgrade and you need to escalate.

To check the system for the maximum number of ports, ask the customer to:

1. Log in to the SAT screen.
2. At the SAT command, `display system-parameters customer-options`.
3. Verify that the **Maximum Ports:** field is 900 or less.

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

During the installation and upgrade procedures, you must back up the system data to an FTP, SCP, or SFTP server.

If you are backing up data over the LAN, you normally use an FTP/SCP/SFTP server on the customer's LAN. To do this, you will need information on how to get to the backup location:

- Login ID and password
- IP address
- Directory path on the FTP server

If necessary, check with your project manager or the customer for this information.



Important:

Before going to the customer site, make sure that you can use either a customer server for backups or a compact flash card.

Obtaining S8300 software and G700 firmware

The files containing the software for the S8300 and the G700 and media module firmware are on the Communication Manager Software Distribution CD-ROM that you take to the site. This CD is called the software CD because it contains software for all of the Linux servers.

Additional files that may be needed are:

- License file
- Authentication file
- Software service pack files (most recent version)
- Security update files
- G700 firmware file (most recent version)

Checking the CD for the most recent firmware files

The firmware on the Communication Manager software distribution CD may not be the most recent. Therefore, check the firmware versions contained on the software CD to verify that you have the latest before installing the firmware using the LSP's TFTP server. You can do this by accessing the CD on your laptop and displaying the actual firmware filenames in the Releases\<release_number>\Gateways directory.

For example, the CD may contain a file mm760v60.fdl, but the most recent firmware available on the Avaya Web site is mm760v65.fdl. In this case, download the mm760v65.fdl file from the Web site for installation instead of installing the file from the CD. As another example, the CD may contain the mgp_25_23_0.bin media gateway file, and the Avaya Web site also contains mgp_25_23_0.bin. In this case, you could use the firmware from the CD because the versions of the files are the same.



CAUTION:

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Obtaining service pack files

Pre- and post-upgrade service packs may be needed for this upgrade. If the service pack files are not on your software CD, download the service pack files from the Avaya Support web site to your laptop.

Pre-upgrade service pack (starting from R2.x only)

This upgrade requires a pre-upgrade service pack. The service pack filename differs, depending on which software load the media server is on. See [Table 38: Pre-Upgrade service pack filenames for software release and load](#) for the software load associated with each release.



CAUTION:

If the customer's system has Release 2.x of Communication Manager but has a field load other than those listed in the table, do not use this section to upgrade Communication Manager to Release 4.0. You must escalate.

Table 38: Pre-Upgrade service pack filenames for software release and load

Software release of existing media server	Associated software load	Service pack filename
Release 2.0	R012x.00.0.219.0	00.0.219.0-xxxx.tar.gz
Release 2.0.1	R012x.00.1.221.1	00.1.221.1-xxxx.tar.gz
Release 2.1	R012x.01.0.411.7	01.0.411.7-xxxx.tar.gz
Release 2.1.1	R012x.01.1.414.1	01.1.414.1-xxxx.tar.gz
Release 2.2	R012x.02.0.111.4	02.0.111.4-xxxx.tar.gz
Release 2.2.1	R012x.02.1.118.1	02.1.118.1-xxxx.tar.gz

Post-upgrade service pack

A post-upgrade service pack may be required. If so, download it from <http://www.avaya.com/support> on the Internet.

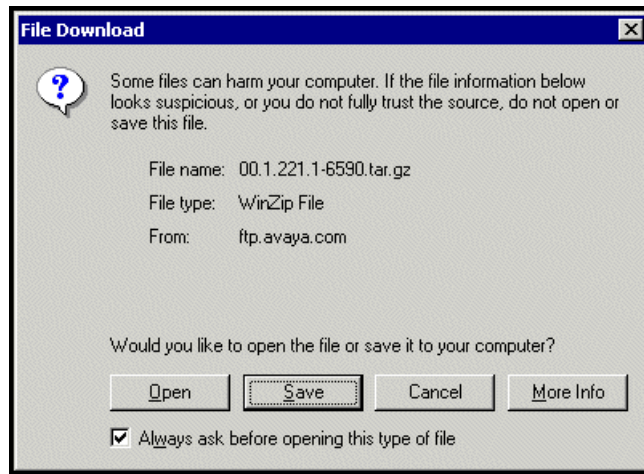
To download service packs to the laptop

1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access <http://www.avaya.com/support> on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At the Avaya support site, click **Downloads**
4. Click on **Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates**.

5. Scroll down to the **Software Update table for Media Servers running Communication Manager**.
6. Click on the link for the appropriate G.A. load.
7. If you are a Business Partner, scroll to the bottom of the page and select **Download Center** to access the password protected Download Center. Otherwise, for Avaya, click on **Latest Avaya Communication Manager x.x.x Service Pack** to access the service pack download

The File Download window displays.

File download window



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

Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary

If IA700 is installed, determine whether a service pack is needed and/or optional languages are used. If so, you will need to obtain the data files.



CAUTION:

This upgrade procedure requires a service interruption of approximately 2 hours, or up to 4 hours if IA770 is being used.

Checking for IA770 stored messages size

When upgrading Communication Manager to release 4.0 from a previous release, the size of the messages stored in IA770 must be less than 72 hours due to a change in the voice encoding algorithm from CELP to G.711. Before the going to the site, have the customer check the size of messages stored in IA770 and, if greater than 72 hours, contact your service support center.

To check the IA770 stored messages size

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **System Configuration and Status > System Status**.

Look for “Used Hours of Speech” in the list. If more than 72 hours is reported, the customer must delete some messages before the upgrade.

Or, you can use the CLI command, `/vs/bin/util/vs_status`.

Obtaining an IA770 service pack file

If an IA770 service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an IA770 service pack file

1. On the Avaya Support Web site, click on **Find Documentation and Downloads by Product Name**.
2. Under the letter "I", select **IA 770 INTUITY AUDIX Messaging Application**.
3. Click on **Downloads**.

To download the IA770 patch software:

4. Click on **IA 770 INTUITY AUDIX Embedded Messaging Application Patches**.
5. Click on the service pack file name for this release.

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

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

Note:

The IA770 patch documentation is co-located with the patch software.

Obtaining optional language files

Optional languages are any language other than English (*us-eng* or *us-tdd*). If optional languages will be used with this IA770, you can also download the appropriate language files from the Download Web site.

1. Follow the steps as in [Obtaining an IA770 service pack file](#) on page 628.
2. At step [4](#), select **IA 770 INTUITY AUDIX Embedded Messaging Application Languages**.

Completing the RFA process (obtaining license and password file)

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

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

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

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

Note:

For an upgrade, you do not normally need to install a new authentication file (with a .pwd extension). However, if one is required, follow the same steps as with a license file.

Downloading license file and Communication Manager versions for an LSP

The license file of the S8300 as a Local Survivable Processor must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300, S8400, S8500, or S8700-series Media Server). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

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

Note:

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

To download the license file to your laptop



Tip:

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

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and authentication files (for example, C:\licenses).
2. Access the Internet from your laptop and go to Remote Feature Activation web site, rfa.avaya.com.
3. Use the System ID, the SAP ID of the customer, or the SAP ID of the switch order to locate the license and authentication files for the customer.
4. Check that the license and authentication files are complete.
You might need to add the serial number of the customer's G700.
5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and authentication files to your laptop.

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

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

Note:

Business Partners call 800-295-0099. ART is available only to Avaya associates.

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

Note:

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

To run the ART

1. Access the ART web site on your laptop at <http://art.dr.avaya.com>.
2. Select **Administer S8x00 Server products for installation script**.
 - a. Log in.
 - b. Enter the customer information.
 - c. Select **Installation Script**.
 - d. Click **Start Installation script & IP Addr Admin**.A script file is created and downloaded or emailed to you.
3. You can use the installation script to set up an IP address and other alarming parameters automatically.

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

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

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

Ensuring a super-user login exists

A super-user login must be administered prior to upgrading the system. The project manager, remote services, or the customer should check to verify that one exists. If a super-user login must be added, you must log in as *dadmin* or a higher level of login. You cannot add the login by logging in as *craft*.

Checking a pre-4.0 release

To ensure that a super-user login exists in Communication Manager prior to Release 4.0:

1. Log in with `telnet` or `ssh`.

- At the SAT command line, enter **list logins**

The Logins screen appears.

```
list logins
```

LOGINS								
Login	Service Level	Status	Pwd. Cycle	Aging (Days)	ASG Blk	Expiration Date	No. of Sess. Sess.	Used
init	init	active			y n	/ /		
inads	inads	inactive			y n	/ /		
dadmin	dadmin	inactive			n n	/ /		
craft	craft	inactive			y n	/ /		
acpsnmp	non-super-user	void			n n	/ /		

- Under the Service Level column, look for a login that has either the dadmin or super-user level.
- If a super-user login does not exist, create one. See [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#) on page 633.

Checking a 4.0 release

To ensure that a super-user login exists in Communication Manager in Release 4.0 or higher:

- Log in with **ssh**.
- At the Linux command line, type **cat /etc/passwd | grep 555**.

The following list of super-user logins appears.

```
init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1001:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash
```

- Look for any logins other than the init, inads, and craft logins. If no additional super-user logins exist, you must create one. See [Creating a super-user login, if necessary, for R4.0 or higher](#) on page 634.

Creating a super-user login, if one does not exist (releases earlier than Release 4.0)

If a super-user login does not exist, one must be added before you can complete the upgrade. The customer or remote services should complete the following task.

1. Use the following steps only if you are starting from a software release *earlier* than Release 4.0:

Note:

Adding a super-user login with the SAT command line requires a dadmin, init, or inads login.

Note:

If you are upgrading an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

2. At the SAT command line, enter add login.

The Login Administration screen appears.

add login
Page 1 of x

LOGIN ADMINISTRATION

Password of Login Making Change:

LOGIN BEING ADMINISTERED

Login's Name:xxxxxxx

Login Type:

Service Level:

Disable Following a Security Violation?

Days to Disable After Inactivity:

Access to INADS Port?

LOGIN'S PASSWORD INFORMATION

Login's Password:

Reenter Login's Password:

Password Aging Cycle Length (Days):

LOGOFF NOTIFICATION

Facility Test Call Notification?

Acknowledgment Required?

Remote Access Notification?

Acknowledgment Required?

ACCESS SECURITY GATEWAY PARAMETERS

Access Security Gateway?

3. In the **Password of Login Making Change** field, type your password.

4. In the **Login's Name** field, type a login name agreed upon with the customer. Alternatively, a Business Partner may add the dadmin login.
5. In the **Login Type** field, type **customer**.
6. In the **Service Level** field, type **super-user**.
7. In the **Days to Disable After Inactivity** field, type **90**.
8. In the **Login's Password** field, type a password.
9. In **Reenter Login's Password** field, type the password again.
10. In the **Password Aging Cycle Length** field, type 90, and press **Enter**.
11. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.
 - a. Log in with `telnet` or `ssh`.
 - b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

Creating a super-user login, if necessary, for R4.0 or higher

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages. Use the following steps only if you are starting from Release 4.0 software or later:

Note:

A craft level login can create a super-user login in Release 4.0 or later.

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

To create a login:

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

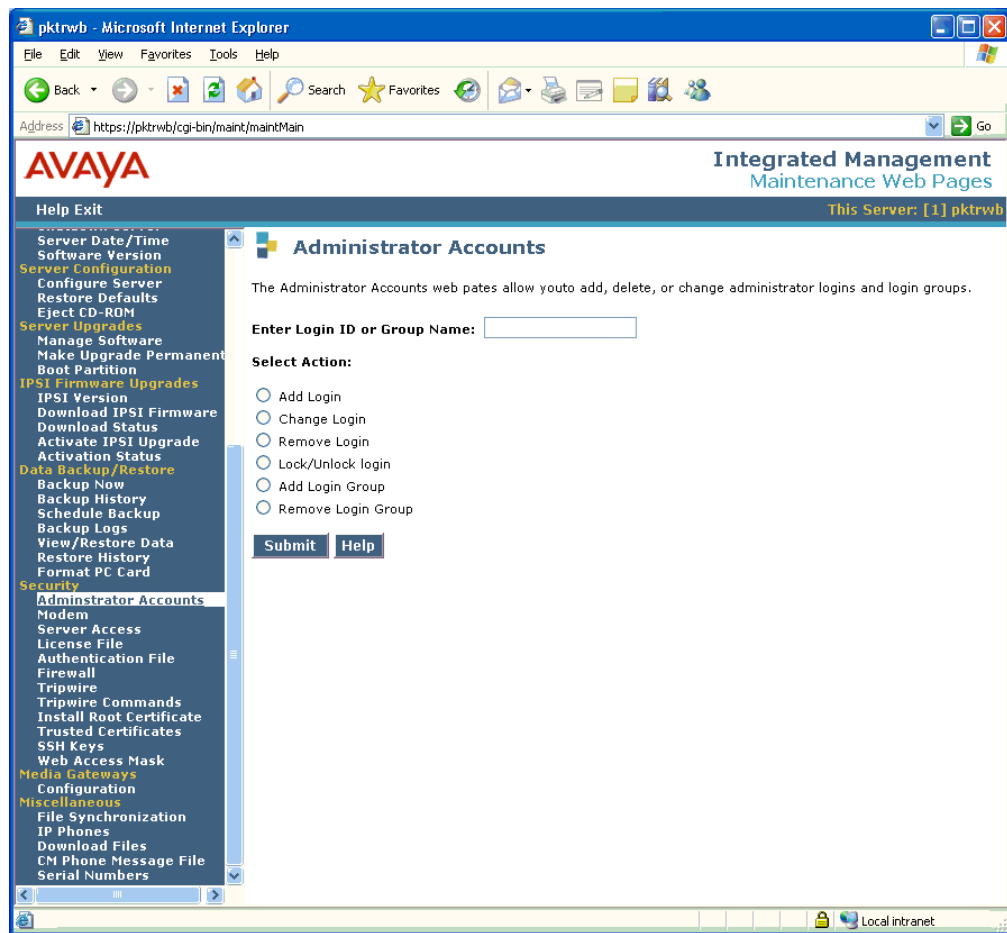
Note:

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

Before going to the customer site

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



3. Type the login name in the **Enter Login ID or Group Name** field.

Manual upgrade of an existing S8300B or S8300C and G700 to R4.0

4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot displays the Avaya Integrated Management Maintenance Web Pages interface. The top header shows the Avaya logo and the title 'Integrated Management Maintenance Web Pages'. Below the header, a navigation menu on the left lists various system management tasks, including 'Restore Defaults', 'Server Upgrades', 'IPSI Firmware Upgrades', 'Data Backup/Restore', and 'Security'. The 'Security' section is expanded, showing 'Administrator Accounts' as the selected option. The main content area is titled 'The Administrator Logins -- Add login web page allows you to add a new administrator login.' and contains the following form fields:

- Login ID:** Pre-filled with 'randy'.
- login group:** Text input field containing 'susers'.
- additional groups:** Text input field containing 'prof18'.
- allow Linux shell access:** Radio button, currently unchecked.
- lock this account:** Radio button, currently unchecked.
- date (YYYY-MM-DD) on which account is disabled (blank to ignore):** Empty text input field.
- select type of authentication:** Radio buttons for 'password' (selected) and 'ASG'.
- enter key or password:** Empty text input field.
- re-enter key or password:** Empty text input field.
- force password/key change on first login:** Radio buttons for 'yes' and 'no' (selected).
- maximum Number of days a password may be used (PASS_MAX_DAYS):** Text input field containing '90'.
- minimum number of days allowed between password changes (PASS_MIN_DAYS):** Text input field containing '90'.
- minimum acceptable password length (PASS_MIN_LEN):** Text input field containing '8'.
- number of days warning given before a password expires (PASS_WARN_AGE):** Empty text input field.
- days after password expires to lock account (0=immediate):** Empty text input field.

At the bottom of the form are 'Add' and 'Help' buttons. The status bar at the very bottom shows 'Done' and 'Internet' connectivity.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

10. Complete the following fields:

- enter a challenge key or password
- re-enter challenge key or password
- force password/key change on first login

Note:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

- a. Log in with `telnet` or `ssh`.
- b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

On-site Preparation for the Upgrade

Perform the following tasks before starting the software upgrade on the S8300.

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See [Laptop configuration for direct connection to the services port](#) on page 42.

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

- [Accessing the server's command line interface with SSH](#) on page 55
- [Logging in to the media server from your laptop using Telnet](#) on page 56
- [Logging in to the S8300 Web Interface from your laptop](#) on page 57

Removing the administration for the IA770 integration if CWY1 board is used

Note:

If the S8300 is configured as an LSP, skip to [Upgrade the S8300](#) on page 657.



CAUTION:

Communication Manager Release 4.0 does not support the CWY1 method of integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current switch integration administration now. You will administer the integration for H.323 after the upgrade.

For instructions on removal of existing CWY1 administration, see *Administering Media Servers to work with IA770*.

Note:

For Releases 2.0 and 2.1 of Communication Manager that use IA770, you *cannot* remove messaging from the Media Gateway screen in the SAT interface *before* the upgrade. Therefore, you must remove messaging from Slot V8 of the Media Gateway screen after the upgrade, then administer the H.323 integration.

Completing pre-upgrade tasks — if the target S8300 is the primary controller

If the S8300 is configured as an LSP, skip to [Upgrade the S8300](#) on page 657.



CAUTION:

If you are upgrading an S8300 primary controller that has LSPs registered to it, the LSPs must be upgraded **before** the primary controller. (You can use the SAT command, `list media-gateway`, to see if there are LSPs registered to the S8300.)

Perform the following procedures if you are upgrading an S8300 that is configured as a primary controller:

- [To display IA770 alarms, if IA770 is enabled](#)
- [To clear alarms](#)
- [To check link status](#)
- [To record all busyouts](#)
- [To disable scheduled maintenance](#)

- [To check for translation corruption](#)
- [To save translations](#)
- [To disable alarm origination](#)

Note:

It is no longer necessary to disable Terminal Translation Initialization (TTI) before an upgrade or to enable it after an upgrade.

To display IA770 alarms, if IA770 is enabled

1. On the Maintenance Web Interface, click **Messaging Administration**.
2. On the Messaging Administration menu, under Logs, click **Alarm**.
3. On the Alarm Log screen, type today's date. Leave the defaults in all other fields.
4. Click Display.
5. Resolve any alarms that are listed.

To clear alarms

1. On the Maintenance Web Interface under Alarms, click **Current Alarms**.
2. If no alarms are listed, skip the next two steps.
3. If alarms are listed, click **Clear All**.
4. Resolve any remaining major alarms through the Communication Manager SAT.

To check link status

1. Open a SAT session.
2. Enter `display communication-interface links`.
Note all administered links.
3. Enter `status link number` for each administered link.
4. Enter `list signaling group`.
Note the signaling groups listed by number.
5. For each of the signaling groups listed, enter `status signaling group number`.
Make a note (write down) of any links that are down.

To record all busyouts

1. At the SAT prompt, type `display errors` and press **Enter**.
2. Look for type 18 errors and record (write down) any trunks that are busied out — you will return them to their busy-out state after the upgrade.

To disable scheduled maintenance

Scheduled daily maintenance must not interfere with the upgrade.

1. At the SAT prompt, type **change system-parameters maintenance** and press **Enter**.
2. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

or,

If scheduled maintenance is not in progress, set the **Start Time** field to a time after the upgrade will be completed.

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

To check for translation corruption

1. At the SAT prompt, type **newterm** and press **Enter**.
2. Enter your terminal type and press **Enter**.

If you see the message,

```
Warning: Translation corruption found
```

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To save translations

1. At the SAT prompt, type **save translation** and press **Enter**.
2. Under **Command Completion Status** you should see *Success*.

To disable alarm origination

If alarm origination is enabled during the upgrade, unnecessary alarms will be sent to the Operations Support System (OSS) destination number(s). Even if you selected **Suppress Alarm Origination** when you logged in, alarm origination will be automatically re-enabled when the system reboots after the software upgrade. Use this procedure to prevent alarm origination from being re-enabled after reboot.



CAUTION:

If you do not disable alarm origination, the system can generate alarms during the upgrade, resulting in unnecessary trouble tickets.

1. Logoff the SAT session.
2. At the command prompt, type **almenable -d n -s n**, where
 - d n sets the dialout option to **neither** (number)
 - s n disables SNMP alarm origination

Note:

Be sure to reset alarm origination after the upgrade.

3. Type **almenable** (without any options) to verify the alarm origination status.

You should see:

```
incoming: enable
```

```
Dial Out Alarm Origination: neither
```

```
SNMP Alarm Origination: n
```

Saving a copy of the 4600-series phone configuration file, if any

During an upgrade, any data in the `/tftpboot` directory is overwritten with new software and firmware. If the system was using the http or tftp capability for 4600-series phone firmware downloads and configuration updates, the firmware and 4600-series phone configuration file are overwritten.

You must redownload the 46xx firmware file after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the `/tftpboot` directory *after* the upgrade.

To copy the 4600-series configuration file to a safe location, perform the following steps:

1. Access the server's command line interface using telnet and an IP address of **192.11.13.6**.
2. Log in as **craft**.
3. At the Linux command line, type **cd /tftpboot**, and press **Enter**.
4. At the prompt, type **ls 46***, and press **Enter**.

If a named **46xxsettings.txt** may appear in the list, or the prompt may reappear with no files listed. If the file name does not appear, there is no file to copy. You are finished with this procedure.

5. If the file name **46xxsettings.txt** appears, at the Linux command line, type **cp 46xxsettings.txt ~ftp/pub**.

The 4600-series phone settings file is now in a protected directory, `/var/home/ftp/pub`, and will not be overwritten during the upgrade. You will copy this file back to the `/tftpboot` directory after the upgrade.

Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used)

Skip to [Backing up S8300 recovery system files](#) on page 647 if IA770 is not being used.

If IA770 is being used, you need to collect optional language data (if this had not been done before arriving at the site), leave a test message, and shut down IA770 before backing up the files.

Determining whether optional languages are needed

To determine the system language

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Global Administration**; then **Messaging Administration**.
3. Enter the *craft* password.
4. At the command prompt, enter **display system-parameters features**.

The **SYSTEM PARAMETERS FEATURES** screen displays.

5. Go to page 3.

System Parameters Features screen

```
redtail          Active          Alarms: none          Logins: 1
display system-parameters features          Page 3 of 4
SYSTEM-PARAMETERS FEATURES

CALL TRANSFER OUT OF AUDIX
Transfer Type: enhanced_cover_0          Transfer Restriction: digits
Covering Extension: 50104

ANNOUNCEMENT SETS
System: us-eng          Administrative:

RESCHEDULING INCREMENTS FOR UNSUCCESSFUL MESSAGE DELIVERY
Incr 1: 0 days 0 hrs 5 mins          Incr 2: 0 days 0 hrs 15 mins
Incr 3: 0 days 0 hrs 30 mins          Incr 4: 0 days 1 hrs 0 mins
Incr 5: 0 days 2 hrs 0 mins          Incr 6: 0 days 6 hrs 0 mins
Incr 7: 1 days 0 hrs 0 mins          Incr 8: 2 days 0 hrs 0 mins
Incr 9: 7 days 0 hrs 0 mins          Incr10: 14 days 0 hrs 0 mins

enter command: display system-parameters features
Cancel Refresh Enter ClearFld Help Choices NextPage PrevPage
```

6. Under **Announcement Sets**, note the main system language listed after **System:** In this example, the main system language is English (**us-eng**). If the system language is anything other than **us-eng** or **us-tdd**, you will need to download the appropriate language files from a language CD after the upgrade.

Note:

Starting with release 2.1, only English language files (**us-eng** and **us-tdd**) are included with the Communication Manager software. Before release 2.1, Latin American Spanish and Canadian French (**lat-span** and **french-c**) were also included.

To determine other languages

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Utilities**; then **Software Management**; then **Messaging System Software Display**.
The **Messaging System Software Display** screen displays.

Messaging System Software Display screen



Avaya IA 770 Intuity™ AUDIX® Messaging
Application
Server Name: 135.9.80.70

High level packages installed on redtail in Package Priority order

audixed	1.3-1.5	Avaya C-Hawk Intuity AUDIX (CHIA) - Versioning Package
websrv	6.0-54	Messaging Web Server Utility Files
CHIAset	6.0-54	Messaging Platform CHIA Set
swmgmt	6.0-48	Software Management
syseval	6.0-48	System Evaluation Utility
C6054rf+a	6.0-54	INTUITY Platform CHIA Set RFU
APPLset	6.0-48	AUDIX(R) Application Set
A6048rf+a	6.0-48	INTUITY Platform APPL Set RFU
us-eng	R7.0-1	US-ENG System Announcements
us-tdd	R7.0-1	US-Tdd System Announcements

[Display software in alphabetical order](#)
[Display software installation time](#)

Indicator meaning:
*** = Package does not match what was installed from the software release.**
+ = Package is in addition to what was installed from the software release.
? = A package within set does not match what was installed from the software release.

[Return to Main](#) [Software Management Menu](#) [Help](#)

3. Note the **System Announcement** language files listed. In this example, **us-eng** and **us-tdd** are listed. If any language files other than these two are listed, you will need to download the additional language files from a language CD after the upgrade.

Downloading optional language files, if needed

Skip to [To shut down IA770 with the command line](#) on page 645 if optional language files are not needed. If the optional language files are needed, copy the files from the language CD to /var/home/ftp/pub.

To download optional language files

1. Insert the optional language CD in your laptop's CD-ROM drive.
2. On the Maintenance Web Interface, under Miscellaneous, select **Download Files**.
3. Select the **Files to download from the machine I'm using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click the **Download** button.

When the transfer is complete, the message

Files have been successfully downloaded to the server

is displayed.

6. If more than four optional language files need to be downloaded, repeat this procedure.

Copies of the optional language files are now in the **/var/home/ftp/pub** directory and will be automatically installed during the upgrade process.

Creating an IA770 test message for the upgrade

To test IA770 after the upgrade

1. Write down the number of a test voice mailbox, or create one if none exists.
2. Write down the number of the IA770 hunt group.
3. Leave a message on the test mailbox that will be retrieved after the upgrade.

Shutting down IA770

To shut down IA770 with the command line

Note:

If you use the Avaya Installation Wizard (IW) to upgrade the server, you would skip this procedure. The IW executes the **stop** command automatically.

1. Type **telnet 192.11.13.6** and press **Enter**.
2. Log in as *craft* or *dadmin*.

3. Type **stop -s Audix** and press **Enter** to shut down AUDIX. Note that the "A" in Audix must be capitalized.

The shutdown will take a few minutes.

4. Type **watch /vm/bin/ss** and press **Enter** to monitor the shutdown.

The watch command will automatically refresh every few seconds. When the shutdown is complete, you will see only the voicemail and audit processes. For example:

voicemail:(10)

audit http:(9)

Press **Ctrl+C** to break out of the **watch** command.

5. Type **/vs/bin/util/vs_status** and press **Enter** to verify that AUDIX is shut down.

When AUDIX is shut down, you will see

voice system is down



Important:

After upgrading an S8300, you must upgrade the G700 or G350 and media module firmware before restarting IA770.

To shut down IA770 with the Maintenance Web pages

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.



Important:

After upgrading an S8300, you must upgrade the G700 and media module firmware before restarting IA770.

Backing up S8300 recovery system files

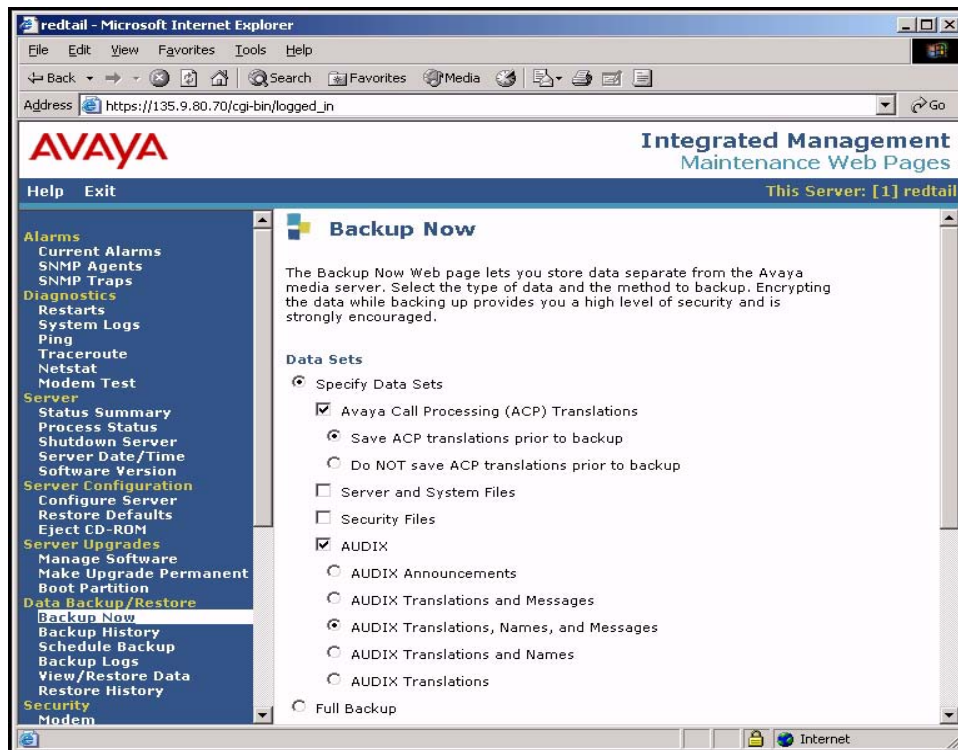
Before installing the S8300 software, back up the system data in case you need to back out of the upgrade. You should back up to an FTP, SFTP, or SCP server on the customer's network. To do this, you need an FTP, SFTP, or SCP address and directory path and a user ID and password to access the customer's network. Check with your project manager or the customer for this information. You can also back up the system data to the S8300 hard drive.

To back up S8300 recovery system data

1. Under Data Backup/Restore, click **Backup Now**.

The **Backup Now** screen displays.

Backup Now screen (Part One)



2. Select **Full Backup**, if available with the existing release, or select all data sets:

- Avaya Call Processing (ACP) Translations
- Save ACP translations prior to backup

Note:

Select ACP translations only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

- Server and System Files
 - Security Files
3. If the AUDIX options are available, select AUDIX and select AUDIX Translations, Names, and Messages.



CAUTION:

Selecting the **Full Backup** radio button does NOT include AUDIX files. You must backup the IA770 INTUITY AUDIX data after you do the full backup.

Backup Now screen (Part Two)

4. Select **Network Device** and then select **FTP** for the backup method and fill in the appropriate fields with information provided by the customer.
5. Click **Start Backup** to back up the files.

Note:

The backup and restore processes use the ping service to check connectivity to the backup server. If a backup or restore operation fails, ensure that the ping service is enabled.

- On the Maintenance Web Interface, under **Security** select **Firewall**.
- In the **Service** column, find **ping**.

The checkboxes for both **Input to Server** and **Output from Server** should be checked.

6. To check the status of the backup:
 - a. Under **Data Backup/Restore**, click **Backup History**.
 - b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

When the backup is finished, the **Backup History Results** screen displays

The final status for your backup job is shown below.

For each backup set, the message

BACKUP SUCCESSFUL

displays, if the set was backed up successfully.

7. If the AUDIX options are available, repeat Steps 3–6 for AUDIX Announcements.

Copying and installing the service pack files to the media server (starting from R2.x only)

Note:

Do not perform this task if you are upgrading an R3.0 release to R4.0.

A pre-upgrade service pack is required to modify the server upgrade tools, including the web Interface and upgrade scripts, which will enable the upgrade to Communication Manager 4.0 to complete successfully.

To copy pre-upgrade service pack file to the media server

1. Insert the software CD in the CD-ROM drive of your laptop.
2. On the Maintenance Web Interface, under Miscellaneous, click **Download Files**.
3. Select the download method, "Files to download from the machine I'm using to connect to the server."

Note:

Do not select the checkbox, "Install this file on the local server."

4. Browse to the directory on the software CD (or laptop) that contains the pre-upgrade service pack file.
5. Select the pre-upgrade service pack file and click **Download**.

To install the pre-upgrade service pack

Note:

Use a telnet session to install and activate the service pack file.

The following steps activate the service pack.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **telnet 192.11.13.6** and press **Enter**.
3. Log in as either **craft** or **dadmin**.
4. Type **update_unpack** and press **Enter**.
5. Select the number corresponding to the service pack file. (For example, **00.0.339.4-xxxx.tar.gz**). Press **Enter**.
6. Type **update_show** and press **Enter** to list Communication Manager files to verify that the new service pack file was unpacked.
7. Type **update_activate update**, where **update** is the release or issue number of the latest service pack file. (For example, **00.0.339.4-xxxx**. Do *not* use the .tar.gz extension at the end of the file name). Press **Enter**.

The media server may reboot. If it reboots, it also may display the message

```
/opt/ecs/sbin/drestart 2 4 command failed.
```

Ignore this message. You must wait until the restart/reset completes before entering additional commands.

The media server displays a message that the service pack was applied.

8. Type **update_show** again and press **Enter** to list Communication Manager files to verify the service pack file was activated.
9. Enter **y** in response to the question, `Commit this software?`

Copying Files to the S8300 hard drive

You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Post-upgrade software service pack
- License file
- Avaya authentication file
- New firmware files
- Security updates
- IA770 service packs or RFUs

To copy files to the S8300 hard drive

1. Under **Miscellaneous** on the Maintenance Web pages, click **Download Files**.

Download Files screen

2. Select "Files to download from the machine I'm using to connect to the server" and browse to each file you want to copy to the S8300. Leave the "Install this file on the local server" checkbox **unchecked**.

If you need to download an IP Telephone firmware file, download this file last with the "Install this file on the local server" checkbox **checked**.

Note:

To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to `pub` after starting ftp and logging in; that is, type `cd pub`.

3. Click on **Download** to copy the files to the S8300. The transfer is complete when you see the message,

Files have been successfully uploaded to the server



Important:

Remove the Communication Manager software distribution CD from the DVD/CD-ROM drive.

Copying the software and firmware files to the server

Normally, during an upgrade, you will have the Communication Manager Software Distribution CD-ROM that contains the latest software to install. The latest software for the S8300 has a file name that reflects the most recent load of software (*For example only*, 013-01.0.640.1). The latest service pack software for Communication Manager also reflects the most recent load of software (*for example only*, 03.1-01.0.640.0).



CAUTION:

When you are upgrading the media server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the media server to a release that is not supported as an upgrade path, you might corrupt the translations.

Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.

To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access <http://support.avaya.com>. Select **Downloads > Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates > Latest Communication Manager Software & Firmware Compatibility Matrix**.

These files also contain the most recent firmware for the G700 Media Gateway, the various media modules, and the P330 Stack Processor.

To transfer files from the software CD

1. Insert the Communication Manager software distribution CD into the CD-ROM drive.
2. Log in to the S8300 Web interface.
3. Under Server Upgrades, click **Manage Software**.

The system displays the **Manage Software** screen.

Manage Software screen

Manage Software

Progress: Choose Task

Choose Task This server is currently running release: **S8300-013-01.0.637.0**

Select the task to perform and click **Continue**.

☐ Copy a release to the local hard drive, but do not install it.

☐ Install one of the following releases currently resident on the local hard drive:

- 03.0-01.0.636.0
- 03.0-01.0.637.0

☐ Delete one of the above releases from the local hard drive.
(This does not affect the release that is running on the system.)

Note: If the web session times out, you can recover by logging in again and clicking the Manage Software link from the menu.

Continue **Cancel** **Help**

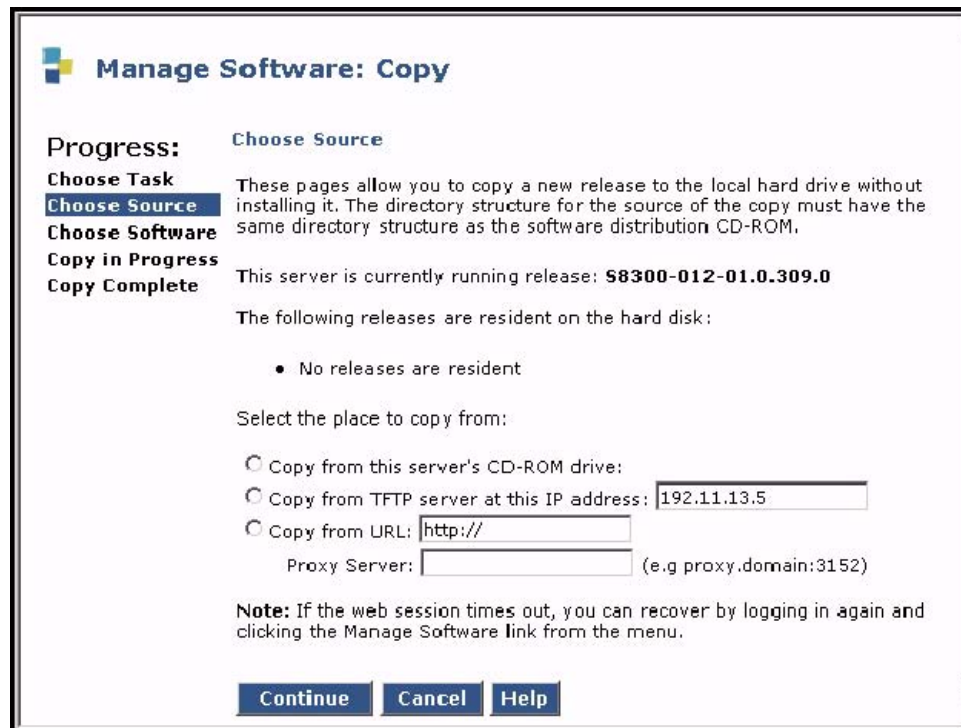
4. Select the radio button **Copy a release to the local hard drive, but do not install it**.

Note:

The S8300 hard drive can hold up to three releases without having to delete a release before copying a new release from the Communication Manager software distribution CD.

The S8300 displays the **Choose Source** screen, which allows you to copy files from one of several possible sources to the S8300 hard drive.

Choose Source screen



The screenshot shows a web interface titled "Manage Software: Copy". On the left is a "Progress:" sidebar with five items: "Choose Task", "Choose Source" (highlighted in blue), "Choose Software", "Copy in Progress", and "Copy Complete". The main content area is titled "Choose Source" and contains the following text: "These pages allow you to copy a new release to the local hard drive without installing it. The directory structure for the source of the copy must have the same directory structure as the software distribution CD-ROM." Below this, it states "This server is currently running release: **S8300-012-01.0.309.0**". Then it says "The following releases are resident on the hard disk:" followed by a bullet point: "• No releases are resident". Next is the instruction "Select the place to copy from:" and three radio button options: "Copy from this server's CD-ROM drive:", "Copy from TFTP server at this IP address: 192.11.13.5", and "Copy from URL: http://". Below the URL field is a "Proxy Server:" field with a placeholder "(e.g proxy.domain:3152)". A "Note:" at the bottom states: "If the web session times out, you can recover by logging in again and clicking the Manage Software link from the menu." At the very bottom are three buttons: "Continue", "Cancel", and "Help".

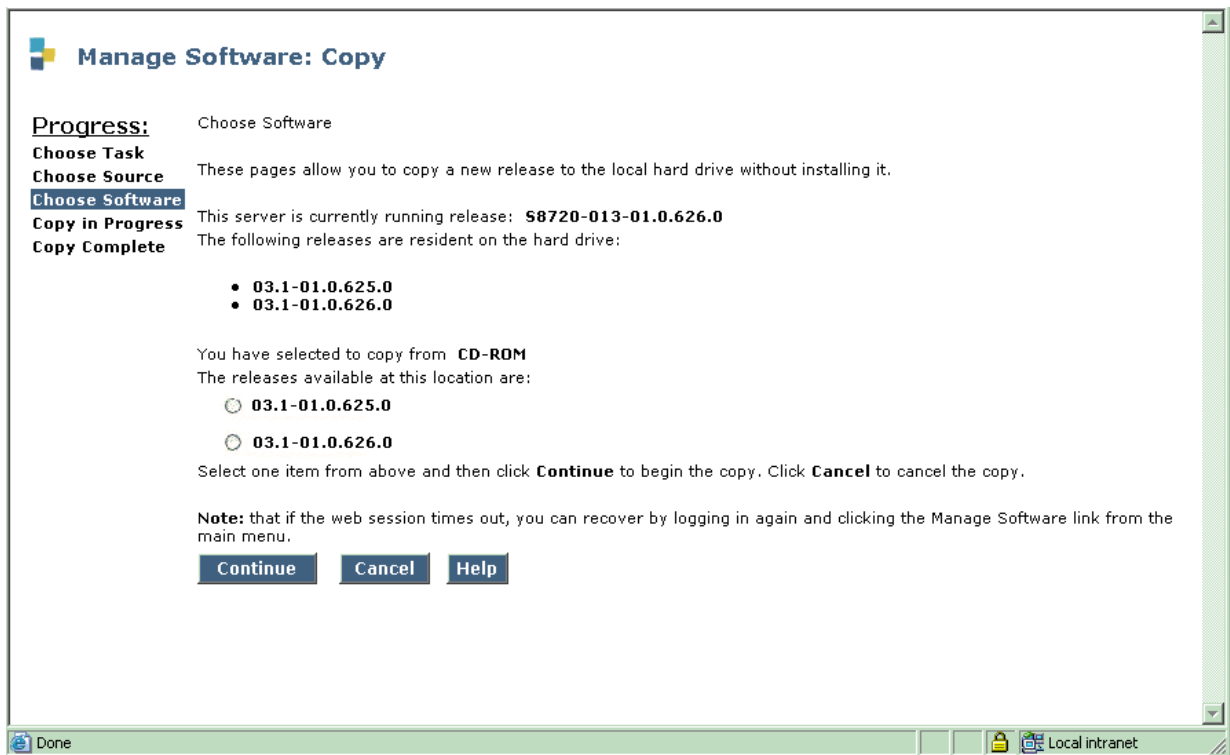
Possible sources include:

- This server's CD-ROM drive
- TFTP server at IP address shown (default is local laptop at 192.11.13.5)
- URL specified in **Copy from URL:** field

If you select the **Copy from this server's CD-ROM drive:** radio button, all available CD drives are checked. The first drive found with a valid release is used, in the event multiple CD drives are actually present.

The system displays the **Choose Software** screen.

Choose Software screen

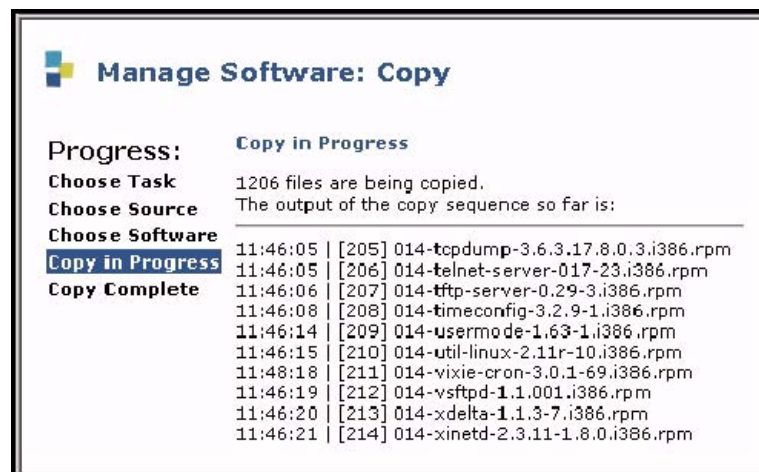


The screen is presented with no radio button selected.

5. Select the release to be copied and click **Continue**.

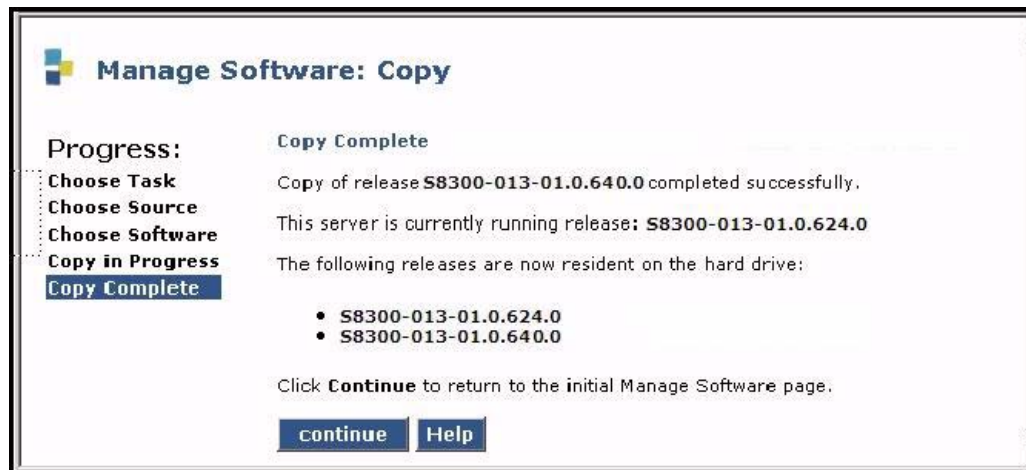
The system displays the **Copy in Progress** screen.

Copy in Progress screen



The screen lists each file as it is being copied to the S8300 hard drive. When the copy completes successfully, the **Copy Complete** screen displays.

Copy Complete screen



This screen indicates the release just copied, shows the release running on the S8300, and shows the releases resident on the server's hard drive.



CAUTION:

At this point you are finished with the software CD-ROM. **Remove the CD from your laptop now** to avoid possible problems the next time your laptop is rebooted.

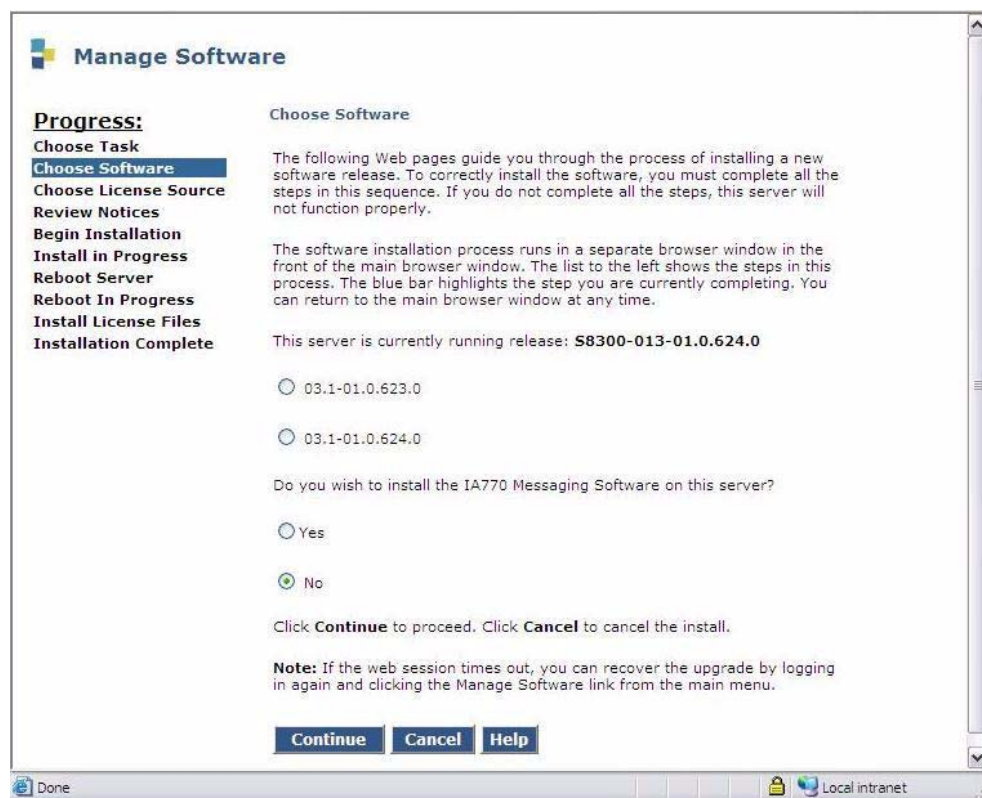
Upgrade the S8300

This section describes the procedures to upgrade the S8300B or S8300C Media Server from a 2.x, 3.x, or 4.0 release of Communication Manager to release 4.x. To upgrade from a pre-2.0, use the procedures in [Chapter 10: Manual upgrade of an S8300A and G700 to R4.0](#).

Installing new software

The first step in upgrading the S8300B or S8300C Media Server to Communication Manager 4.x is to copy the appropriate software release to the server hard drive using the Manage Software screens of the Web Interface (see [Copying the software and firmware files to the server](#) on page 652). The next step is installation of that release, which is now resident on the S8300B hard drive, onto the S8300 Media Server. After you have finished with the **Copy Complete** screen, click **Continue**. The **Choose Software** of the **Manage Software: Install** screen displays.

Choose Software screen



This screen will show the release currently running on the S8300, and the releases resident on the hard drive. To install the 4.x release, click the radio button next to the 4.x release and click **Continue**.

This screen also displays a prompt for installing IA770 INTUITY AUDIX Messaging.

The radio buttons default as follows: If IA770 is not supported, the "no" button will be selected; if IA770 is supported, the "yes" button will be selected.

The install screens following the IA770 screen are unchanged from their former versions.

1. Click **Continue**.

The S8300 displays the **Choose License Source** screen.

Choose License Source screen

Manage Software

Progress:

- Choose Task
- Choose Software
- Choose License Source**
- Review Notices
- Begin Installation
- Install in Progress
- Reboot Server
- Reboot In Progress
- Install License Files
- Installation Complete

Choose License Source

You must have a software license file before you install this software release. If you do not have this file available, use tools in the main window to transfer it to the system. DO NOT continue this installation until it is available.

Select a source for the license files:

- ☒ I will supply the license files myself when prompted later in this process.
- ☐ I want to reuse the license files from the currently active partition on this server.

It is not normally necessary to update the authentication information, but if the new software documentation instructs you to, you may update it as well.

- ☐ Do not update authentication information.
- ☒ Update authentication information as well as license information.

Click **Continue** to proceed. Click **Cancel** to cancel the install.

Note: that if the web session times out, you can recover the upgrade by logging in again and clicking the Manage Software link from the main menu.

Continue **Cancel** **Help**

2. If you have installed the license and authentication files, select the following:

- I want to reuse the license files from the currently active partition on this server.
- Do not update authentication information.

For a normal installation, the license and authentication files should have been installed at this point. If these files have not been installed, select the following:

- I will supply the license/authentication files myself when prompted later in this process.
- Update authentication information as well as license information.

3. Click **Continue**.

The system displays the **Review Notices** screen.

4. For a new installation, or if you previously ran a backup, you do not need to run a backup at this time.

If your planning documents instruct you to enable Tripwire, follow the instructions to reset the signature database.

5. Click **Continue**.

The S8300 displays the **Begin Installation** screen, which summarizes the request you have made.

6. Click **Continue**.

The S8300 displays the **Install in Progress** screen.

7. The installation should take 10 to 20 minutes.

The **Install in Progress** screen refreshes every 10 seconds or on demand by clicking the **Refresh** button. When complete, the S8300 displays the **Reboot Server** screen.

8. Click **Reboot**.

If IA770 is being used, it may take approximately 5 minutes to shut down IA770 before the reboot begins.

The S8300 displays the **Reboot in Progress** screen.

Note:

The reboot can take 20 minutes or longer. The system does not automatically tell you when the reboot is complete.

Wait 5 minutes and then click **Continue**. If you click **Continue** before the reboot is finished, the screen will display **Expired Page**. If you see the **Expired Page** message, refresh the browser. If the **Session Timeout** screen appears, close the screen, logoff, and log on again. Click the **Pickup** button.

If IA770 is being installed when you click **Continue** and you get the **Expired Page** message, enter the 192.11.13.6 URL in the address window of your browser. When you log in you will be able to monitor the IA770 installation progress.

Note:

This Web session will be interrupted by the reboot which occurs during the upgrade of the primary server. After the reboot, you can continue to use the **Manage Software** window without logging in.

9. When the reboot is complete, clicking **Continue** will display the **Update Tripwire Database** screen.
10. Unless instructed in your planning documents to update the tripwire database, select **Do not update the tripwire data base now** and click **Continue**.

The system displays the **Installation Complete** screen.

11. Click **Close**.

You are returned to the main menu.

Note:

This Web session will be interrupted by the reboot that occurs during the primary server upgrade. After the reboot, the links in the main menu of the Web interface will not function. Therefore, you must close and reopen the Web browser to continue with the upgrade procedure.

12. Close the Web browser.
13. Reopen the Web browser and log in.
14. Under Server, click **Software Version** to verify the new software version.



Important:

After upgrading an S8300, you must upgrade the G700 or G350 and media module firmware before restarting IA770.

Installing updated authentication files



CAUTION:

A super-user login, dadmin or another customer superuser login, must exist *before* you install an authentication file. If the authentication file does not install, you might need to create a super-user login, then install the new authentication file. See [Ensuring a super-user login exists](#) on page 631.

To install the license and authentication files:

1. On the Maintenance Web Interface menu under Security, select **License File**.

The **License File** screen displays.

License File Screen

License File

The License File Web page allows installation of Avaya license files.

CommunicMgr License Mode: Normal
 Network used for License: Carrier MCP
 License Serial Number is 01DR12310260 on carrier MCP

☐ Undo last install
☒ Install the license file I previously downloaded
☐ Install the license file specified below

File Path

URL

Proxy Server e.g proxy.domain:3152)

2. Select **Install the license file I previously downloaded** and click **Submit**.

The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.

4. The **Authentication File** screen displays.

Authentication File screen

Authentication File

The Authentication File Web page allows installation of Avaya authentication files.

☒ Install the Authentication file I previously downloaded
☐ Install the Authentication file I specified below

File Path

URL

Proxy Server (e.g. proxy.domain:3152)

5. Select **Install the Authentication file I previously downloaded** and click **Install**.

The system tells you the authentication file is installed successfully. If the authentication file does not install, you may need to add a super-user login first. See [Ensuring a super-user login exists](#) on page 631.

If upgrading an LSP, synchronize translations from the primary controller

If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

1. Log in with `telnet` or `ssh`.
2. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

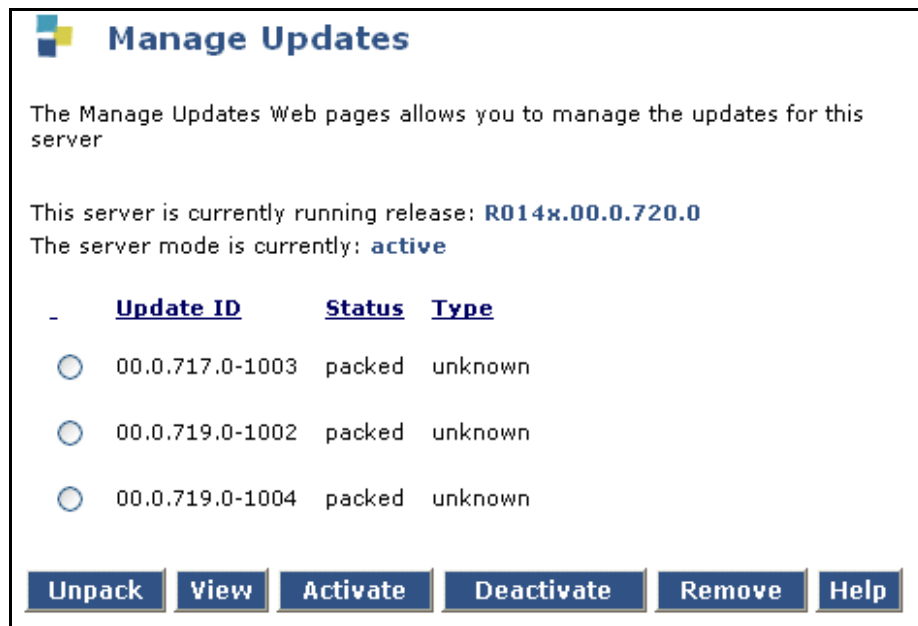
1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`
3. Type `start -ca`

Installing security and Communication Manager service pack updates, if any

To install update files

1. Under Server Upgrades, select **Manage Updates**.
The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allows you to manage the updates for this server

This server is currently running release: **R014x.00.0.720.0**
 The server mode is currently: **active**

	<u>Update ID</u>	<u>Status</u>	<u>Type</u>
☐	00.0.717.0-1003	packed	unknown
☐	00.0.719.0-1002	packed	unknown
☐	00.0.719.0-1004	packed	unknown

Unpack View Activate Deactivate Remove Help

- If an update file you want to activate shows **packed** in the **Status** column, select update ID and click **Unpack**.

The window shows the status of the unpacking.

- Wait until the system displays the message **Finished unpacking...** and click **Continue**.

The system displays the **Manage Updates** screen.

- If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

- Click **Yes**.

Wait until the system displays the Continue button.

- Click **Continue**.

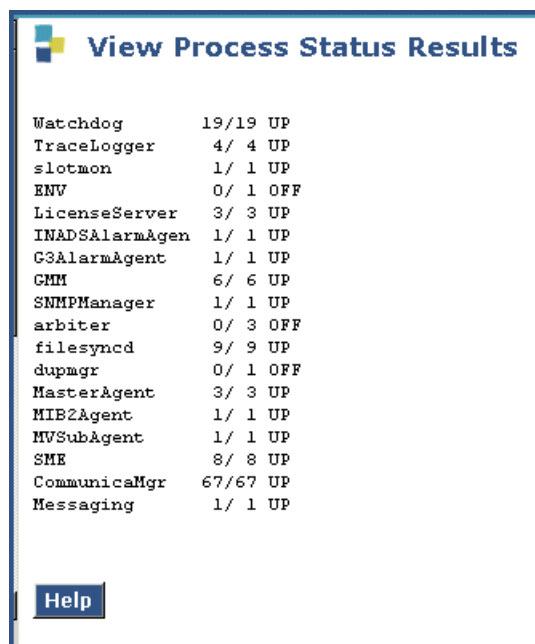
If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started

If you installed IA770 INTUITY AUDIX Messaging, the messaging application should start after you install the license. To verify that messaging has started, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

the **View Process Status Results** screen displays.

View Process Status screen



View Process Status Results		
Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicMgr	67/67	UP
Messaging	1/ 1	UP

Help

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

If you need to start messaging, you can use either the Maintenance Web pages or the Linux command line. For the Maintenance Web pages, see [Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary](#) on page 665. For the Linux command line method, see [Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary](#) on page 665.

Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary

1. From the Maintenance Web Page, select **Messaging Administration** from the **Miscellaneous** menu.

The Messaging Administration Web page is displayed in a new Web browser window.

2. From the Messaging Administration Web page, select **Utilities**.

The Utilities Web page is displayed.

3. Select **Start Messaging Software**.

The Start Messaging Software Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

2. Type `start -s Audix`

3. Ensure that all Communication Manager processes come up.

To monitor the startup of IA770:

- a. Type `watch /VM/bin/ss`

The display will periodically refresh automatically. When you see the following display, the IA770 startup is complete.

- b. Press **Ctrl+C** to break out of the `watch` command.

If IA 770 fails to start after an upgrade

If you have upgraded your Communication Manager and IA 770 INTUITY AUDIX software, you must have a new license that is associated with the latest release. IA 770 will not use the license for a previous version.

If you upgraded IA 770 without a new license file, it will fail to start during the Communication Manager startup sequence.

If this occurs, you must do the following steps:

1. Obtain an IA 770 Replace variable w/ release number license file.
2. Install the license file.
3. From a command prompt, start the IA 770 process with the following command:

```
start -s Audix
```

Test to verify system functionality

Test the system for functionality by verifying the following:

- Telephones have dial tone
- You can call from one telephone to another telephone on the system
- You can make an external trunk call.
- The media gateways have registered. Use the SAT command `list media-gateway`.

Making the upgrade permanent



CAUTION:

You must make the upgrade of the software permanent so that the software is recognized and kept on the S8300. If you fail to make software permanent, then the next time you reboot, old software will become active.

To make the upgrade permanent

1. From the Maintenance Web Interface main menu, under Server Upgrades click **Make Upgrade Permanent**.

The S8300 displays the **Make Upgrade Permanent** window.

2. Click **Submit**.

When the new S8300 upgrade software is permanent, the S8300 displays the message:

The commit operation completed successfully

Saving translations

Note:

If the S8300 you are upgrading is an **LSP**, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session. and log in as *craft* (or *dadmin*).
2. If the S8300 you are upgrading is a primary controller, at the SAT prompt, type **save translation** and press **Enter**.
3. If the S8300 you are upgrading is an LSP, then on the primary controller, type **save translation lsp** and press **Enter**. This command distribute saved translations out to the LSPs.

When the save is finished, the system displays the message,

Command successfully completed.

The system automatically performs a reset system 4. If you are upgrading an LSP, you are logged out.

Copying IP Phone firmware to the media server, if necessary

If, before the upgrade, the server was serving as an http server for IP phone firmware, download the most recent IP phone firmware bundle available from the Avaya Firmware Download Web site. The firmware bundle reinstates the 46xx IP Phone Web page in Communication Manager and also makes the 46xx IP Phone firmware for the tftp or http server capability of the media server.

Note:

The IP phone firmware that was originally downloaded will have been overwritten.

To copy files to the media server:

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

The files are copied automatically to the /tftpboot directory. The 46xx IP Phone Web page is reinstated at the next reboot.

Restoring the 4600-series phone configuration file, if any

If you copied a 4600-series phone configuration file to the `/var/home/ftp/pub` directory prior to the upgrade, you should restore it after the upgrade. However, before you restore the file, be sure you have downloaded the appropriate IP phone firmware.

1. At the Linux command line, type `cd ~ftp/pub`, and press **Enter**.
2. At the prompt, type `cp 46xxsettings.txt /tftpboot`, and press **Enter**.

The 4600-series phone settings file is now restored to the `/tftpboot` directory.

Upgrade the G700 Firmware

This section describes how to upgrade firmware on the components of the G700, including the Media Gateway Processor (MGP), the P330 Stack Processor, and any installed media modules.

Verifying the contents of the `tftpboot` directory

Before proceeding with the G700 firmware installation, you should check the `/tftpboot` directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the `/tftpboot` directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.



CAUTION:

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the `/var/home/ftp/pub` directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the `pub` directory.

3. Copy the firmware files from the `pub` directory to the `/tftpboot` directory, using the S8300 Media Server command line interface.

To copy firmware files to the `/tftpboot` directory of an S8300 Media Server, do the following:

- a. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.

- b. Log in as craft.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to /var/home/ftp/pub.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the /tftpboot directory. To copy multiple firmware files (most firmware files have an .fdl suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the /tftpboot directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to /tftpboot.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

Conduct the following procedure to compare software versions running on the G700 processors and media modules with the versions in you planning documents. If the versions do not match, you need to install the new firmware for those components.

To determine if new firmware for the P330 stack processor is necessary

1. Access the stack processor. See one of the following:
 - [Logging in to the P330 Stack Processor with a Direct Connection to the S8300 Services Port](#) on page 62
 - [Logging in to the P330 Stack Processor with a LAN Connection](#) on page 63
 - [Logging in to the P330 Stack Processor with a Direct Serial Connection](#) on page 64
 - [Logging in to the P330 Stack Processor with Device Manager](#) on page 64
2. At either the **P330-1(super)#** or **P330-1(configure)#** prompt, type `dir`.
The system displays the directory list of software for the P330 stack processor.

Directory list for P300 stack processor

M#	file	ver num	file type	file location	file description
--	----	-----	-----	-----	-----
1	module-config	N/A	Running Conf	Ram	Module
	Configuration				
1	stack-config	N/A	Running Conf	Ram	Stack Configuration
1	EW_Archive	4.0.4	SW Web Image	NV-Ram	WEB Download
1	Booter_Image	3.2.5	SW BootImage	NV-Ram	Booter Image

3. Check the version number (ver num) of the EW_Archive file to see if it matches the Release Letter.

If not, you must upgrade the P330 stack processor.

4. Type **show image version**

The system displays the list of software.

Show image version List for P330 stack processor

Mod	Module-Type	Bank	Version
-----	-----	----	-----
3	Avaya G700 media gateway	A	0.0.0
3	Avaya G700 media gateway	B	4.0.17

5. Check the version number of the stack software image file in Band B to see if it matches the your planning document.

If not, you must upgrade the P330 stack processor.

To determine if new firmware is required for the MGP, VoIP module, and installed media modules

1. Type **session mgp**
2. At the **MG-001-1(super)#** prompt, type **show mg list_config**

The system displays the list of software.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (B)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

3. Refer to the list to check the FW vintage number of the G700.

In the TYPE column, find G700, then check the matching field in the FW VINTAGE column to see if it matches the vintage number in your planning forms. If not, you must install new firmware on the G700 media gateway. Also check if the release number in the FW VINTAGE column contains (A) or (B) to designate the software bank. If the list shows B, you will upgrade A. If the list shows A, you will upgrade B.

4. Refer to the VOIP FW column and row for slot V0 (same row occupied by the G700 information) to see if the number matches the VoIP firmware identified in your planning forms.

If not, you must also upgrade the G700 media gateway motherboard VoIP module.

Note:

The VoIP processor on the motherboard is upgraded using the same firmware image file as the VoIP media modules; for example, the file mm760v8.fdl is vintage #8.

5. Check the FW VINTAGE column for vintages of each of the installed media modules: MM710, MM711, MM712, MM720, and/or MM760 to see if they match the FW vintages in the planning forms.

If not, you must upgrade them, as well.

Installing new firmware on the P330 stack processor

To Install P330 stack processor firmware

1. From your S8300 telnet session, telnet back to the P330 stack processor:

Type `telnet <xxx.xxx.xxx.xxx>`,

where `<xxx.xxx.xxx.xxx>` is the IP address of the P330 stack master processor on the customer's LAN.

2. At the **P330-1(configure)#** prompt, type

```
copy tftp SW_image <file> EW_archive <ew_file>
<tftp_server_address> <Module#>
```

where `<file>` is the full-path name for the image file with format and vintage number similar to viisa3_8_2.exe,

`<ew_file>` is the full-path name for the embedded web application file with format similar to p330Tweb.3.8.6.exe,

`<tftp_server_ip_address>` is the IP address of the TFTP server, and

`<Module#>` is the number, 1 through 10, of the media gateway in the stack. If there is only one G700 media gateway, the number is 1.

3. Verify that the download was successful when the prompt returns:
 - a. type `show image version <module #>` and check the version number in the Version column for Bank B.
 - b. type `dir <module #>` and check the version number in the ver num column for the EW_Archive file.
4. Type `reset <module #>`.

Installing new firmware on the G700 Media Gateway Processor

To install MGP firmware

1. At the **P330-1(configure)#** prompt, type `session mgp` to reach the G700 media gateway processor.
2. Type `configure` at the **MG-???-1(super)#** prompt to enter configuration mode, which will change the prompt to **MG-???-1(configure)#**.
3. At the **MG-???-1(configure)#** prompt, type `show mgp bootimage` to determine which disk partition (bank) is in the **Active Now** column.

You will update the bank that is *not* listed as Active Now. The system displays the following screen:

Example: Show mgp bootimage

<u>FLASH MEMORY</u>	<u>IMAGE VERSION</u>
Bank A	109
Bank B	210
<u>ACTIVE NOW</u>	<u>ACTIVE AFTER REBOOT</u>
Bank B	Bank B

4. At the **MG-???-1(configure)#** prompt, type
`copy tftp mgp-image <bank> <filename> <tftp_server_ip_address>`
to transfer the mgp image from the tftp server to the G700,
where
<bank> is the bank that is *not* Active Now (Bank A in the example).
<filename> is the full path name of the mgp firmware image file, which begins with mgp and will be similar to the name mgp_8_0.bin.
<tftp_server_ip_address> is the IP address of the S8300.
For example:
`copy tftp mgp-image a mgp_8_0.bin 195.123.49.54`
The screen shows the progress.

5. Type `set mgp bootimage <bank>`

where *<bank>* is the same letter you entered in the previous step.

6. At the **MG-???-1(configure)#** prompt, type `reset mgp`.

A system prompt asks you to confirm the reset.

7. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

8. When the **P330-1(super)#** prompt appears, type `session mgp`.

9. At the **MGP-???-1(super)#** prompt, type `configure`.

10. Verify that the download was successful when the prompt returns.

Type `show mg list_config`.

The system displays the list of software.

Example: Show mg list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
V0	G700	DAF1	A	00	230 (A)	67
V1	ICC	S8300	A	72	00	N/A
V2	DCP	MM712	A	2	58	N/A
V3	ANA	MM711	A	2	57	N/A
V4	DS1	MM710	A	1	58	N/A

Installing new firmware on the media modules

For upgrades of active media modules, you need to take the media modules out of service before initiating the upgrade process. To do this, go to a SAT session on the primary controller and issue a `busyout` command.

Note:

Skip this busyout procedure if the media modules are not in service; for example during an initial installation.

To busyout board (for active media modules)

1. Go to a SAT session on the primary controller and enter the command,

`busyout board vx`

where *x* is the slot number of the media module to be upgraded.

2. Verify the response,

Command Successfully Completed

3. Repeat for each media module to be upgraded.

To install media module firmware

1. Be sure that you have checked for the current vintage of the VoIP Module for the v0 slot (on the G700 motherboard).

This VoIP module does not occupy a physical position like other media modules.

2. At the **P330-1(configure)#** prompt, type **session mgp**.
3. At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.
4. Type **copy tftp mm-image v<slot #> <filename mm> <tftp_server_ip_address>**

where

<slot #> is the slot of the specific media module,

<filename mm> the full-path name of the media module firmware file in a format such as mm712v58.fdl, and

<tftp_server_ip_address> is the ip address of the S8300.

Two or three minutes will be required for most upgrades. The VoIP media module upgrade takes approximately 5 minutes. Screen messages indicate when the transfer is complete.

5. After you have upgraded all the media modules, verify that the new versions are present.

At the **MG-???-1(configure)#** prompt, type **show mg list_config**

The list of software appears.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (A)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

6. In the **TYPE** column, find the particular media module (v1 through v4), then check the matching field in the **FW VINTAGE** column to see if it matches the planning documentation.

Note:

Slot V1 can contain either a media module or the S8300, which will show as
TYPE ICC.

7. Check the **VOIP FW** column and row for slot v0 to see if the number matches the VoIP firmware identified in the planning documentation.
8. Type **reset <module #>**
where **<module #>** is the number of the G700 in the stack.
9. When the reset is finished, type **show mm** to verify the upgrade.

To release board (if media module was busied out)

1. When the upgrade procedure is complete, go to the SAT session and release the board

Type **release board vx**

where **x** is the slot number of the upgraded media module.

2. Verify the response,

Command Successfully Completed

Note:

If you see the response, Board Not Inserted, this means that the media module is still rebooting. Wait one minute and repeat the **release board** command.

3. Repeat the **release board** command for each media module that was busied out.

Ensuring the MGP default gateway IP address is set

Communication Manager release 4.0 requires that the built-in VoIP module of the G700 Media Gateway has a default gateway IP address. To ensure that this IP address is set, perform the following steps:

1. At the **MG-???-1(configure)#** prompt, type **show ip route mgp**.

The list of mgp routes appears.

MG-001-1(super)# show ip route mgp				
DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	135.9.80.254	motfec0	(3/0/165)
135.9.80.0	255.255.255.0	135.9.80.88	motfec0	(101/0/0)
MG-001-1(super)#				

2. Check that a Gateway IP address exists for Destination 0.0.0.0.

3. If a Gateway IP address does not exist, type, at the **MG-???-1(configure)#** prompt, **set ip route 0.0.0.0 0.0.0.0 <IP_address>**, where **<IP_address>** is the default gateway IP address.

After you reboot the media gateway, the IP address is active and available.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 stack processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* (available at <http://www.avaya.com/support>).

Installing new firmware on other G700 media gateways

Installing G700 firmware in a stack configuration

If the customer has multiple G700 media gateways connected in an IP stack, you can stay connected to the master G700/P330 and "session" over from the master P330 Stack Processor to the next G700 in the stack. If you are dialed in remotely, you should have automatically dialed in to the stack master. For a local installation, you should have plugged your laptop into the stack master P330, which you can identify by the LED panel on the upper left of each G700 or P330 device in the stack.

The LEDs signal as follows:

- On the G700 Media Gateway: a lit **MSTR** LED indicates that this unit is the stack master.
- On the P330 device: a lit **SYS** LED indicates that this unit is the stack master.

The G700 and P330 at the bottom of the stack is module number 1, the next module up is number 2, and so on. However, the stack master can be any module in the stack, depending on the actual model, the vintage firmware it runs, and whether the S8300 is inserted into it.

Note:

You do not need to configure the other P330 processors in the stack. These will use the IP address and IP route of the master stack processor. However, you will need to check firmware on all devices of the other G700s in the stack, including the media gateways themselves, and update the firmware as required.

You may also use the "session stack" command to access other standalone P330 processors in the stack (those that are not part of a G700 unit).

To "session" over to another G700/P330 in a stack

1. At the **MG-001-1(configure)#** prompt, type `session stack`

The **P330-1(configure)#** prompt appears.

2. At the **P330-1(configure)#** prompt, type `session <mod_num> mgp`

where `<mod_num>` is the next P330 processor in the stack.

If you are currently logged in to the master stack processor, `<mod_num>` would be `2`, for the second G700/P330 processor in the stack.

3. For other G700s in the stack, repeat the steps described previously to install firmware for the stack processor, MGP, and media modules.

Installing G700 firmware in a remote, no stack configuration

If additional G700 media gateways are supported in the configuration, but they are not attached as a stack, then you must configure each G700, with all of its devices, including the P330 processors. Additionally, you must check firmware and update the firmware as required.

Post-upgrade tasks

After the upgrade is complete, perform the following post-upgrade tasks.

Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update

After the upgrade is complete, perform the following post-upgrade tasks.

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing IA770 service pack (or RFU) files, if any

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at <http://support.avaya.com>.

1. Select **Messaging Administration** from the main menu.
2. Select **Utilities** from the Messaging Administration menu.
3. Select **Software Management** from the Utilities menu.
4. Select **Advanced Software Installation** from the Software Management menu.
5. Select **Continue this operation without current system backup**.
6. Select the IA770 update package and click **Install Selected Packages**.

Note:

The system automatically prompts you to restart INTUITY AUDIX when the service pack has been installed. Therefore, if you restart AUDIX at this time, you do *not* need to perform the following procedure, [Starting IA770 INTUITY AUDIX Messaging](#).

Starting IA770 INTUITY AUDIX Messaging

**CAUTION:**

You do *not* need to perform this task if you restarted AUDIX as a part of the installation of the IA770 service pack.

After the IA770 INTUITY AUDIX Messaging application has been updated, you must restart it using the following steps:

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Start Messaging Software**.

The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

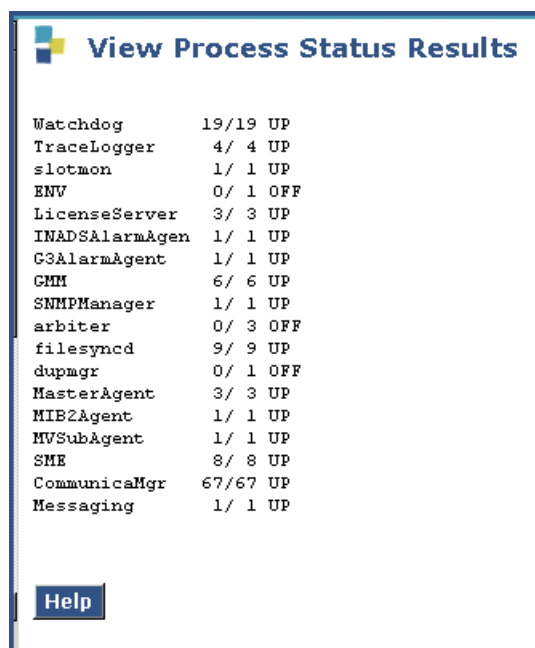
Verifying start up of IA770 INTUITY AUDIX Messaging

To verify operation of IA770 INTUITY AUDIX Messaging, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

the **View Process Status Results** screen displays.

View Process Status screen



Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

[Help](#)

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an IA770 sanity test:
 - a. At the Linux command line, type `/vs/bin/display`
 - b. All states should be `Inserv` with an associated phone number.
 - c. Retrieve the test message saved before the upgrade.

Saving translations

To save translations:

1. In the SSH session, open a SAT session.
2. Log in again as *craft*.

3. Type **save translation** and press **Enter**.

When the save is finished, the system displays the message,
Command successfully completed.

If using IA770, administering switch integration for H.323

The IA770 INTUITY AUDIX Messaging application uses H.323 signaling instead of the CWY1 board for integration with Communication Manager. The tasks for administering the H.323 integration are explained in *Administering Media Servers to work with IA770*.

Testing to verify system functionality

Test the system for functionality, if you are upgrading an S8300 primary controller;

1. Verify the following:
 - Telephones have dial tone
 - You can call from one telephone to another telephone on the system
 - You can make an external trunk call.
 - The media gateways have registered. Use the SAT command **list media-gateway**.

Completing the upgrade process (S8300 is the primary controller)

Telnet to the S8300 (primary controller) and open a SAT session:

1. [To check media modules](#) on page 682
2. [To enable scheduled maintenance](#) on page 682
3. [To busy out trunks](#) on page 682
4. [To check for translation corruption](#) on page 682
5. [To resolve alarms](#) on page 682
6. [To re-enable alarm origination](#) on page 683
7. [Backing up the system](#) on page 683

To check media modules

1. Type `list configuration all` and press **Enter**.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that Communication Manager is working.

To enable scheduled maintenance

1. Type `change system-parameters maintenance` and press **Enter**.
2. Ensure that the **Start Time** and **Stop Time** fields' administration is the same as before the upgrade.

To busy out trunks

1. Busy out trunks that were busied out before the upgrade (see [To record all busyouts](#) on page 639).

To check for translation corruption

1. Type `newterm` and press **Enter**.

If you do not get a login prompt and see the following message:

```
Warning: Translation corruption detected
```

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To resolve alarms

1. On the Maintenance Web Interface, under Alarms click **Current Alarms** to examine the alarm log.
2. If any alarms are listed, click **Clear All**.
3. Resolve new alarms since the upgrade through Communication Manager using the appropriate maintenance book.

To re-enable alarm origination

1. Telnet to the S8300 and log on.
2. At the command prompt, type `almenable -d b -s y`,
where
 - d b sets the dialout option to *both* (numbers)
 - s y enables SNMP alarm origination
3. Type `almenable` (without any options) to verify alarm origination enabled status.

Backing up the system

To back up the system over the customer's LAN

1. Make sure you have the IP address of the customer's FTP, SFTP, or SCP backup server.
2. On the S8300 main menu, select **Backup Now**.
 The system displays the **Backup Now** screen.
3. Select the type of data you want to back up by selecting the appropriate data set.
4. Select a backup method, normally **FTP**, **SFTP**, or **SCP**, to indicate the destination to which the system sends the backup data.
5. Complete the following fields:
 - **User name**
 You must enter a valid user name to enable the media server to log in to the FTP or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.
 - **Password**
 You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.
 - **Host name**
 Enter the DNS name or IP address of the FTP or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).
 - **Directory**
 Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. The default directory for backup data on the FTP or SCP server is `/var/home/ftp`. If you do not want to use the default directory, you must enter the path name for the directory.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

This completes the installation of the G700 Media Gateway with an S8300 Media Server as primary controller.

Chapter 12: Manual upgrade of an existing S8300B and G700 to S8300C with R4.0

This chapter covers the procedures to replace an S8300B with an S8300C and upgrade the software from a 2.x or 3.x release to 4.0. The procedures to upgrade the G700 firmware use CLI commands instead of the Upgrade Tool. This chapter also covers the procedures to upgrade the firmware on an installed Avaya G700 Media Gateway.



Important:

This chapter assumes that the currently installed S8300 is version B, which is required to run Communication Manager release 2.0 or greater. If the currently installed S8300 is version A, follow the upgrade procedures in [Chapter 10: Manual upgrade of an S8300A and G700 to R4.0](#)

Considerations for upgrading the S8300B as a primary controller or as an LSP

The S8300 can be configured as either the primary controller or as a local survivable processor (LSP). When the S8300 is an LSP, the primary controller, running Avaya Communication Manager, can be either another S8300 or an S8400, S8500, or S8700-series Media Server.

 CAUTION:

When you are upgrading the media server as a primary controller, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for the supported upgrade paths. If you attempt to upgrade the media server to a release that is not supported as an upgrade path, you might corrupt the translations.

Also, you must check **Latest Communication Manager Software & Firmware Compatibility Matrix** for compatibility of software loads between the primary controller and any LSPs or ESSs. If the software loads of the primary controller and the LSPs/ESSs are incompatible, then file synchronization between the primary controller and the LSPs/ESSs can cause translation corruption on the LSPs/ESSs.

To check the **Latest Communication Manager Software & Firmware Compatibility Matrix** from any computer, access <http://support.avaya.com>. Select **Downloads > Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates > Latest Communication Manager Software & Firmware Compatibility Matrix**.

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

- The version of Communication Manager running on the LSP must be exactly the same as, or a later version that is compatible to, the version running on the primary controller.
- If upgrading both the primary controller and the LSP to the same release, you must upgrade the LSP first. Then, with Communication Manager turned off on the LSP, you upgrade the primary controller.

Converting the integration of IA770 INTUITY AUDIX Messaging from CWY1 to H.323

 CAUTION:

Communication Manager Release 4.0 does not support the CWY1 integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current IA770 integration administration before the upgrade and then administer the integration to H.323 after the upgrade.

For instructions on converting the integration to H.323, including the removal of existing administration, see *Administering Media Servers to work with IA770*, 07-600788.



CAUTION:

Be sure to test the new integration before completing the upgrade.

The need to restore IP Phone files

During an upgrade, any data in the /tftpboot directory is overwritten with new software and firmware. If the system was using the http or tftp capability for 4600-series phone firmware downloads and configuration updates, the firmware and 4600-series phone configuration file are overwritten.

You must retrieve the 46xx firmware (the 46xx .tar file, for example **46xxH323_cm2_2_wi1_15_ip2_2_111405.tar**) from the Avaya Downloads Web site and download the 46xx firmware file to the server after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the /tftpboot directory *after* the upgrade. See the following:

- [Saving a copy of the 4600-series phone configuration file, if any](#) on page 704
- [Copying IP Phone firmware to the media server, if necessary](#) on page 739
- [Restoring the 4600-series phone configuration file, if any](#) on page 740

Tasks to upgrade the S8300B to S8300C on release 4.0 and upgrade the G700 firmware

The major tasks to upgrade the S8300B to release 4.0 and upgrade the G700 firmware are:

Before going to the customer site

- [Getting information that the project manager provides](#) on page 690
- [Getting the serial number of the G700, if necessary](#) on page 690
- [Checking the number of allocated ports](#) on page 690
- [Checking the availability of the FTP, SFTP, or SCP server for backing up data](#) on page 691
- [Obtaining S8300 software and G700 firmware](#) on page 691
- [Obtaining service pack files, if needed](#) on page 692
- [Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary](#) on page 693
- [Completing the RFA process \(obtaining license and password file\)](#) on page 694
- [Running the Automatic Registration Tool \(ART\) for the INADS IP address, if necessary](#) on page 696

- [Ensuring a super-user login exists](#) on page 697
- [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#) on page 698

On-site Preparation for the Upgrade

- [Accessing the S8300](#)
- [Removing the administration for the IA770 integration if CWY1 board is used](#)
- [Completing pre-upgrade tasks — If the target S8300 is the primary controller](#)
- [Saving a copy of the 4600-series phone configuration file, if any](#)
- [Getting IA770 \(AUDIX\) Data and Stopping IA770 \(if IA770 is being used\)](#)
- [Determining whether optional languages are needed](#)
- [Checking for any IA770 custom announcement sets](#)
- [Creating an IA770 test message for the upgrade](#)
- [Shutting down IA770](#)
- [Backing up S8300 recovery system files](#)
- [Recording configuration information](#)

Upgrade the S8300

- [Replacing the S8300B with the S8300C Media Server](#)
- [Remastering the hard drive and installing the software](#)
- [Verifying Software Version](#)
- [Copying Files to the S8300 hard drive](#)
- [Downloading optional language files, if needed](#)
- [Installing security and Communication Manager service pack updates, if any](#)
- [Setting the Time, Date, and Time Zone](#)
- [Configuring network parameters](#)
- [Verifying connectivity](#)
- [Disabling RAM disk on the media server](#)
- [Rebooting the media server](#)
- [Restoring all data](#)
- [Enabling RAM disk on the media server](#)
- [Rebooting the media server](#)
- [Installing updated license and authentication files](#)
- [Creating a super-user login, if necessary, for R4.0 or higher](#)

- [If the server is an LSP, stop and start Communication Manager](#)
- [If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started](#)
- [Copying IP Phone firmware to the media server, if necessary](#)
- [Restoring the 4600-series phone configuration file, if any](#)

Upgrade the G700 Firmware

- [Verifying the contents of the tftpboot directory](#)
- [Determining which firmware to install on the G700](#)
- [Installing new firmware on the P330 stack processor](#)
- [Installing new firmware on the G700 Media Gateway Processor](#)
- [Installing new firmware on the media modules](#)
- [Setting rapid spanning tree on the network](#)
- [Installing new firmware on other G700 media gateways](#)

Post-upgrade tasks

- [If using IA770, administering switch integration for H.323](#)
- [Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update](#)
- [Installing IA770 service pack \(or RFU\) files, if any](#)
- [Starting IA770 INTUITY AUDIX Messaging](#)
- [Verifying start up of IA770 INTUITY AUDIX Messaging](#)
- [Saving translations](#)
- [Testing to verify system functionality](#)
- [Completing the upgrade process \(S8300 is the primary controller\)](#)
- [Backing up the system](#)

Before going to the customer site

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

Obtaining a USB DVD/CD-ROM drive

Upgrading Communication Manager on an S8300 to release 4.0 requires remastering the S8300B/C hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on an external USB CD-ROM drive (S8300B or S8300C). Therefore, you must have a USB DVD/CD-ROM drive at the site.

Getting information that the project manager provides

Ask the project manager for the information needed to prepare for this installation. [Appendix B: Information checklists](#) provides several checklists to help you gather the installation and upgrade information.

Getting the serial number of the G700, if necessary

To get the serial number of the G700 Media Gateway, ask the customer's administrator to:

1. Log in to the S8300 Maintenance web pages.
2. Select **View License Status** or **License File** from the main menu to display the serial number.

Note:

The serial number should also be on a sticker on the back of the G700 chassis, but this number is occasionally incorrect.

Checking the number of allocated ports

Release 4.0 of Communication Manager supports a maximum of 900 ports if the S8300 is a primary controller. If the existing system has more than 900 ports allocated, then there may be a problem with the upgrade and you need to escalate.

To check the system for the maximum number of ports, ask the customer to:

1. Log in to the SAT screen.
2. At the SAT command, `display system-parameters customer-options`.
3. Verify that the **Maximum Ports:** field is 900 or less.

Checking the availability of the FTP, SFTP, or SCP server for backing up data

During the installation and upgrade procedures, you must back up the system data to an FTP, SFTP, or SCP server. You use a server on the customer's LAN for backups. A current version of the system data is required to restore the system configuration upon completion of the upgrade.

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



Important:

Before going to the customer site, make sure that you can use a customer server over the LAN for backups.

Obtaining S8300 software and G700 firmware

The files containing the software for the S8300 and the G700 and media module firmware are on the Communication Manager Software Distribution CD-ROM that you take to the site. This CD is called the software CD because it contains software for all of the Linux servers.

Additional files that may be needed are:

- License file
- Authentication file
- Software service pack files (most recent version)
- Security update files
- G700 firmware file (most recent version)

Checking the CD for the most recent firmware files

The firmware on the Communication Manager software distribution CD may not be the most recent. Therefore, check the firmware versions contained on the software CD to verify that you have the latest before installing the firmware using the LSP's TFTP server. You can do this by accessing the CD on your laptop and displaying the actual firmware filenames in the Releases\<release_number>\Gateways directory.

For example, the CD may contain a file mm760v60.fdl, but the most recent firmware available on the Avaya Web site is mm760v65.fdl. In this case, download the mm760v65.fdl file from the Web site for installation instead of installing the file from the CD. As another example, the CD may contain the mgp_25_23_0.bin media gateway file, and the Avaya Web site also contains mgp_25_23_0.bin. In this case, you could use the firmware from the CD because the versions of the files are the same.



CAUTION:

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Obtaining service pack files, if needed

Post-upgrade service packs may be needed for this upgrade. If the service pack files are not on your software CD, download the service pack files from the Avaya Support web site to your laptop.

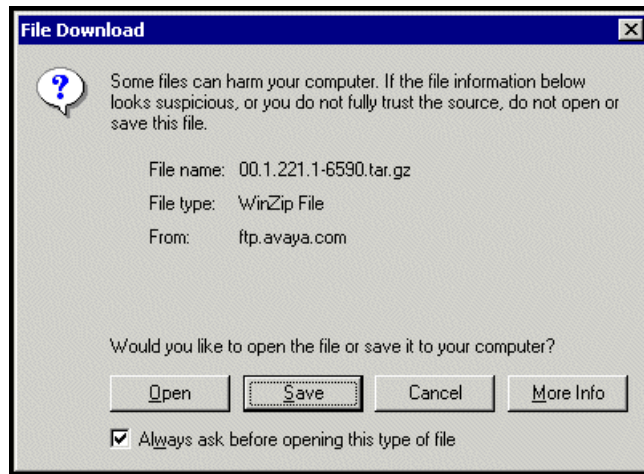
A post-upgrade service pack may be required. If so, download it from <http://www.avaya.com/support> on the Internet.

To download service packs to the laptop

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

The File Download window displays.

File download window



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

Obtaining service pack and language files for IA770 INTUITY AUDIX Messaging, if necessary

If IA700 is installed, determine whether a service pack is needed and/or optional languages are used. If so, you will need to obtain the data files.

CAUTION:

This upgrade procedure requires a service interruption of approximately 2 hours, or up to 4 hours if IA770 is being used.

Checking for IA770 stored messages size

When upgrading Communication Manager to release 4.0 from a previous release, the size of the messages stored in IA770 must be less than 72 hours due to a change in the voice encoding algorithm from CELP to G.711. Before the going to the site, have the customer check the size of messages stored in IA770 and, if greater than 72 hours, contact your service support center.

To check the IA770 stored messages size

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.

2. Select **System Configuration and Status > System Status**.

Look for “Used Hours of Speech” in the list. If more than 72 hours is reported, the customer must delete some messages before the upgrade.

Or, you can use the CLI command, `/vs/bin/util/vs_status`.

Obtaining an IA770 service pack file

If an IA770 service pack is required after the upgrade, obtain the service pack file from the Avaya Support web site.

To obtain an IA770 service pack file

1. On the Avaya Support Web site, click on **Find Documentation and Downloads by Product Name**.
2. Under the letter "I", select **IA 770 INTUITY AUDIX Messaging Application**.
3. Click on **Downloads**.

To download the IA770 patch software:

4. Click on **IA 770 INTUITY AUDIX Embedded Messaging Application Patches**.
5. Click on the service pack file name for this release.

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

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

Note:

The IA770 patch documentation is co-located with the patch software.

Obtaining optional language files

Optional languages are any language other than English (**us-eng** or **us-tdd**). If optional languages other than English are used for announcements, you will need to download the optional languages from a language CD after the upgrade. Before going to the site, obtain the appropriate language CDs or determine that they are available at the site.

Completing the RFA process (obtaining license and password file)

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

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

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

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

Note:

For an upgrade, you do not normally need to install a new authentication file (with a .pwd extension). However, if one is required, follow the same steps as with a license file.

Downloading license file and Communication Manager versions for an LSP

The license file of the S8300 as a Local Survivable Processor must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300, S8400, S8500, or S8700-series Media Server). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

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

Note:

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

To download the license file to your laptop



Tip:

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

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

You might need to add the serial number of the customer's G700.

5. If the files are not complete, complete them.
6. Use the download or E-mail capabilities of the RFA web site to download the license and authentication files to your laptop.

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

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

Note:

Business Partners call 800-295-0099. ART is available only to Avaya associates.

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

Note:

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

To run the ART

1. Access the ART web site on your laptop at <http://art.dr.avaya.com>.
2. Select **Administer S8x00 Server products for installation script**.
 - a. Log in.
 - b. Enter the customer information.
 - c. Select **Installation Script**.
 - d. Click **Start Installation script & IP Addr Admin**.

A script file is created and downloaded or emailed to you.

3. You can use the installation script to set up an IP address and other alarming parameters automatically.

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

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

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

Ensuring a super-user login exists

A super-user login must be administered prior to upgrading the S8300 Media Server. The project manager, remote services, or the customer should check to verify that one exists. If a super-user login must be added, you must log in as dadmin or a higher level of login. For pre-4.0 releases, you cannot add the login by logging in as craft.



Important:

The Communication Manager Web pages for the upgrade might time out if too much time elapses without activity. In this case, you might not be able to log in again with the craft login. This problem can occur after you install the new media server and restore translations and security files, but *before* you install the new authentication file. In such a case, you also cannot login with other higher-level services logins such as INADS. However, you *can* relogin with the customer's super-user login, if it exists. Then you can install the new authentication file and complete the upgrade.

Therefore, it is critical that you ensure that a super-user login exists before you perform the upgrade. In addition, you should retrieve the super-user login and password from the customer prior to performing the upgrade.

Checking a pre-4.0 release

To ensure that a super-user login exists in Communication Manager prior to Release 4.0:

1. Log in with **telnet** or **ssh**.
2. At the SAT command line, enter **list logins**

The Logins screen appears.

list logins									
LOGINS									
Login	Service Level	Status	Pwd. Cycle	Aging (Days)	ASG	Blk	Expiration Date	No. of Sess. Sess.	Used
init	init	active			y	n	/ /		
inads	inads	inactive			y	n	/ /		
dadmin	dadmin	inactive			n	n	/ /		
craft	craft	inactive			y	n	/ /		
acpsnmp	non-super-user	void			n	n	/ /		

3. Under the Service Level column, look for a login that has either the dadmin or super-user level.

4. If a super-user login does not exist, create one. See [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#).

Checking a 4.0 release

To ensure that a super-user login exists in Communication Manager in Release 4.0 or higher:

1. Log in with **ssh**.
2. At the Linux command line, type **cat /etc/passwd | grep 555**.

The following list of super-user logins appears.

```
init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1001:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash
```

3. Look for any logins other than the init, inads, and craft logins. If no additional super-user logins exist, you must create one. See [Creating a super-user login, if one does not exist \(releases earlier than Release 4.0\)](#).

Creating a super-user login, if one does not exist (releases earlier than Release 4.0)

If a super-user login does not exist, one must be added before you can complete the upgrade. The customer or remote services should complete the following task.

1. Use the following steps only if you are starting from a software release *earlier* than Release 4.0:

Note:

Adding a super-user login with the SAT command line requires a dadmin, init, or inads login.

Note:

If you are upgrading an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the **filesync -a <IP_address_of_LSP>** command.

2. At the SAT command line, enter add login.

The Login Administration screen appears.

add login	Page 1 of x
LOGIN ADMINISTRATION	
Password of Login Making Change:	
LOGIN BEING ADMINISTERED	
Login's Name:xxxxxxx	
Login Type:	
Service Level:	
Disable Following a Security Violation?	
Days to Disable After Inactivity:	
Access to INADS Port?	
LOGIN'S PASSWORD INFORMATION	
Login's Password:	
Reenter Login's Password:	
Password Aging Cycle Length (Days):	
LOGOFF NOTIFICATION	
Facility Test Call Notification?	Acknowledgment Required?
Remote Access Notification?	Acknowledgment Required?
ACCESS SECURITY GATEWAY PARAMETERS	
Access Security Gateway?	

3. In the **Password of Login Making Change** field, type your password.
4. In the **Login's Name** field, type a login name agreed upon with the customer. Alternatively, a Business Partner may add the dadmin login.
5. In the **Login Type** field, type **customer**.
6. In the **Service Level** field, type **super-user**.
7. In the **Days to Disable After Inactivity** field, type **90**.
8. In the **Login's Password** field, type a password.
9. In **Reenter Login's Password** field, type the password again.
10. In the **Password Aging Cycle Length** field, type 90, and press **Enter**.
11. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.
 - a. Log in with **telnet** or **ssh**.
 - b. At the Linux command line, type **filesync -a <IP_address_of_LSP>**, where **<IP_address_of_LSP>** is the IP address of the LSP you are upgrading.

On-site Preparation for the Upgrade

Perform the following tasks before starting the software upgrade on the S8300:

Accessing the S8300

To perform the installation and upgrade procedures you will need to connect your laptop to the S8300 Services port using a crossover cable. For a direct connection to the S8300 Services port, your laptop must be properly configured. See [Laptop configuration for direct connection to the services port](#) on page 42.

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

- [Accessing the server's command line interface with SSH](#) on page 55
- [Logging in to the S8300 Web Interface from your laptop](#) on page 57

Note:

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

Removing the administration for the IA770 integration if CWY1 board is used

Note:

If the S8300 is configured as an LSP, skip to [Upgrade the S8300](#) on page 712.



CAUTION:

Communication Manager Release 4.0 does not support the CWY1 method of integration of IA770 INTUITY AUDIX Messaging. As a result, if the S8300 Media Server uses a CWY1 board to integrate the IA770 INTUITY AUDIX application, you must remove the current switch integration administration now. You will administer the integration for H.323 after the upgrade.

For instructions on removal of existing CWY1 administration, see *Administering Media Servers to work with IA770*.

Note:

For Releases 2.0 and 2.1 of Communication Manager that use IA770, you *cannot* remove messaging from the Media Gateway screen in the SAT interface *before* the upgrade. Therefore, you must remove messaging from Slot V8 of the Media Gateway screen after the upgrade, then administer the H.323 integration.

Completing pre-upgrade tasks — If the target S8300 is the primary controller

 CAUTION:

If you are upgrading an S8300 primary controller that has LSPs registered to it, the LSPs must be upgraded **before** the primary controller. (You can use the SAT commands, `list media-gateway` or `list survivable-processor`, to see if there are LSPs registered to the S8300.)

Perform the following procedures if you are upgrading an S8300 that is configured as a primary controller:

- [To display IA770 alarms, if IA770 is enabled](#)
- [To clear alarms](#)
- [To check link status](#)
- [To record all busyouts](#)
- [To disable scheduled maintenance](#)
- [To check for translation corruption](#)
- [To save translations](#)
- [To disable alarm origination](#)

Note:

It is no longer necessary to disable Terminal Translation Initialization (TTI) before an upgrade or to enable it after an upgrade.

To display IA770 alarms, if IA770 is enabled

1. On the Maintenance Web Interface, click **Messaging Administration**.
2. On the Messaging Administration menu, under Logs, click **Alarm**.
3. On the Alarm Log screen, type today's date. Leave the defaults in all other fields.
4. Click Display.
5. Resolve any alarms that are listed.

To clear alarms

1. On the Maintenance Web Interface under Alarms, click **Current Alarms**.
2. If no alarms are listed, skip the next two steps.
3. If alarms are listed, click **Clear All**.
4. Resolve any remaining major alarms through the Communication Manager SAT.

To check link status

1. Open a SAT session.
2. Enter `display communication-interface links`.
Note all administered links.
3. Enter `status link number` for each administered link.
4. Enter `list signaling group`.
Note the signaling groups listed by number.
5. For each of the signaling groups listed, enter `status signaling group number`.
Make a note (write down) of any links that are down.

To record all busyouts

1. At the SAT prompt, type `display errors` and press **Enter**.
2. Look for type 18 errors and record (write down) any trunks that are busied out — you will return them to their busy-out state after the upgrade.

To disable scheduled maintenance

Scheduled daily maintenance must not interfere with the upgrade.

1. At the SAT prompt, type `change system-parameters maintenance` and press **Enter**.
2. If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.

or,

If scheduled maintenance is not in progress, set the **Start Time** field to a time after the upgrade will be completed.

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

To check for translation corruption

1. At the SAT prompt, type **newterm** and press **Enter**.
2. Enter your terminal type and press **Enter**.

If you see the message,

```
Warning: Translation corruption found
```

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To save translations

1. At the SAT prompt, type **save translation** and press **Enter**.
2. Under **Command Completion Status** you should see `Success`.

To disable alarm origination

If alarm origination is enabled during the upgrade, unnecessary alarms will be sent to the Operations Support System (OSS) destination number(s). Even if you selected **Suppress Alarm Origination** when you logged in, alarm origination will be automatically re-enabled when the system reboots after the software upgrade. Use this procedure to prevent alarm origination from being re-enabled after reboot.

**CAUTION:**

If you do not disable alarm origination, the system can generate alarms during the upgrade, resulting in unnecessary trouble tickets.

1. Logoff the SAT session.
2. At the command prompt, type **almenable -d n -s n**, where
 - d n sets the dialout option to **neither** (number)
 - s n disables SNMP alarm origination

Note:

Be sure to reset alarm origination after the upgrade.

3. Type **almenable** (without any options) to verify the alarm origination status.

You should see:

```
incoming: enable
```

```
Dial Out Alarm Origination: neither
```

```
SNMP Alarm Origination: n
```

Saving a copy of the 4600-series phone configuration file, if any

During an upgrade, any data in the `/tftpboot` directory is overwritten with new software and firmware. If the system was using the http or tftp capability for 4600-series phone firmware downloads and configuration updates, the firmware and 4600-series phone configuration file are overwritten.

You must redownload the 46xx firmware file after the upgrade. However, you can save a copy of the 46xx configuration file *before* the upgrade and copy it back into the `/tftpboot` directory *after* the upgrade.

To copy the 4600-series configuration file to a safe location, perform the following steps:

1. Access the server's command line interface using telnet and an IP address of `192.11.13.6`.
2. Log in as `craft`.
3. At the Linux command line, type `cd /tftpboot`, and press **Enter**.
4. At the prompt, type `ls 46*`, and press **Enter**.

If a named `46xxsettings.txt` may appear in the list, or the prompt may reappear with no files listed. If the file name does not appear, there is no file to copy. You are finished with this procedure.

5. If the file name `46xxsettings.txt` appears, at the Linux command line, type `cp 46xxsettings.txt ~ftp/pub`.

The 4600-series phone settings file is now in a protected directory, `/var/home/ftp/pub`. The customer must use FTP to copy the file to a laptop or FTP server.

Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used)

Skip to [Backing up S8300 recovery system files](#) on page 708 if IA770 is not being used.

If IA770 is being used, you need to collect optional language data (if this had not been done before arriving at the site), leave a test message, and shut down IA770 before backing up the files.

Determining whether optional languages are needed

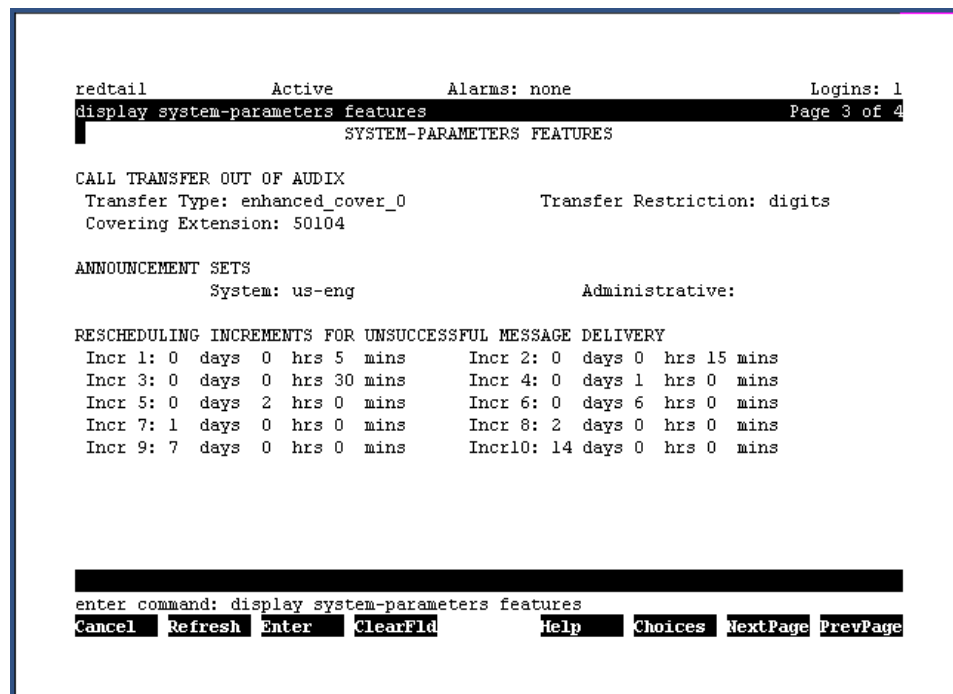
To determine the system language

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Global Administration**; then **Messaging Administration**.
3. Enter the *craft* password.
4. At the command prompt, enter **display system-parameters features**.

The **SYSTEM PARAMETERS FEATURES** screen displays.

5. Go to page 3.

System Parameters Features screen



```

redtail           Active           Alarms: none           Logins: 1
display system-parameters features           Page 3 of 4
SYSTEM-PARAMETERS FEATURES

CALL TRANSFER OUT OF AUDIX
Transfer Type: enhanced_cover_0           Transfer Restriction: digits
Covering Extension: 50104

ANNOUNCEMENT SETS
System: us-eng           Administrative:

RESCHEDULING INCREMENTS FOR UNSUCCESSFUL MESSAGE DELIVERY
Incr 1: 0 days 0 hrs 5 mins           Incr 2: 0 days 0 hrs 15 mins
Incr 3: 0 days 0 hrs 30 mins           Incr 4: 0 days 1 hrs 0 mins
Incr 5: 0 days 2 hrs 0 mins           Incr 6: 0 days 6 hrs 0 mins
Incr 7: 1 days 0 hrs 0 mins           Incr 8: 2 days 0 hrs 0 mins
Incr 9: 7 days 0 hrs 0 mins           Incr10: 14 days 0 hrs 0 mins

enter command: display system-parameters features
Cancel Refresh Enter ClearFld Help Choices NextPage PrevPage

```

6. Under **Announcement Sets**, note the main system language listed after **System:** In this example, the main system language is English (**us-eng**). If the system language is anything other than **us-eng** or **us-tdd**, you will need to download the appropriate language files from a language CD after the upgrade. Also, if the language is a custom set, you must change the name to **us-eng** or **us-tdd**. See [Checking for any IA770 custom announcement sets](#) on page 707.

Note:

Starting with release 2.1, only English language files (**us-eng** and **us-tdd**) are included with the Communication Manager software. Before release 2.1, Latin American Spanish and Canadian French (**lat-span** and **french-c**) were also included.

To determine other languages

1. On the Maintenance Web Interface, under Miscellaneous select **Messaging Administration**.
2. Select **Utilities**; then **Software Management**; then **Messaging System Software Display**.

The **Messaging System Software Display** screen displays.

Messaging System Software Display screen

AVAYA

Avaya IA 770 Intuity™ AUDIX® Messaging Application
Server Name: 135.9.80.70

High level packages installed on redtail in Package Priority order

audixed	1.3-1.5	Avaya C-Hawk Intuity AUDIX (CHIA) - Versioning Package
websrv	6.0-54	Messaging Web Server Utility Files
CHIAset	6.0-54	Messaging Platform CHIA Set
swmgmt	6.0-48	Software Management
syseval	6.0-48	System Evaluation Utility
C6054rft+a	6.0-54	INTUITY Platform CHIA Set RFU
APPLset	6.0-48	AUDIX(R) Application Set
A6048rft+a	6.0-48	INTUITY Platform APPL Set RFU
us-eng	R7.0-1	US-ENG System Announcements
us-tdd	R7.0-1	US-Tdd System Announcements

[Display software in alphabetical order](#)
[Display software installation time](#)

Indicator meaning:
* = Package does not match what was installed from the software release.
+ = Package is in addition to what was installed from the software release.
? = A package within set does not match what was installed from the software release.

[Return to Main](#) [Software Management Menu](#) [Help](#)

3. Note the **System Announcement** language files listed. In this example, **us-eng** and **us-tdd** are listed. If any language files other than these two are listed, you will need to download the additional language files from a language CD after the upgrade.

Checking for any IA770 custom announcement sets

When you restore announcement sets, Communication Manager looks for standard names for the announcement sets. Therefore, if a custom announcement set exists, check with the customer to ensure that the customer wants to restore it. If the set is to be restored, you must change the name of the set to a standard name, either **us-eng** or **us-tdd**.

In this case, do the following:

1. Add a name for the standard announcements backup set, for example, **us-eng-backup**.
2. Copy the standard announcements from the standard set, for example **us-eng**, to the backup set.
3. Copy the announcements of the custom announcement set into the announcement set with the standard name.

Creating an IA770 test message for the upgrade

To test IA770 after the upgrade

1. Write down the number of a test voice mailbox, or create one if none exists.
2. Write down the number of the IA770 hunt group.
3. Leave a message on the test mailbox that will be retrieved after the upgrade.

Shutting down IA770

To shut down IA770

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.



Important:

After upgrading an S8300, you must upgrade the G700 and media module firmware before restarting IA770.

Backing up S8300 recovery system files

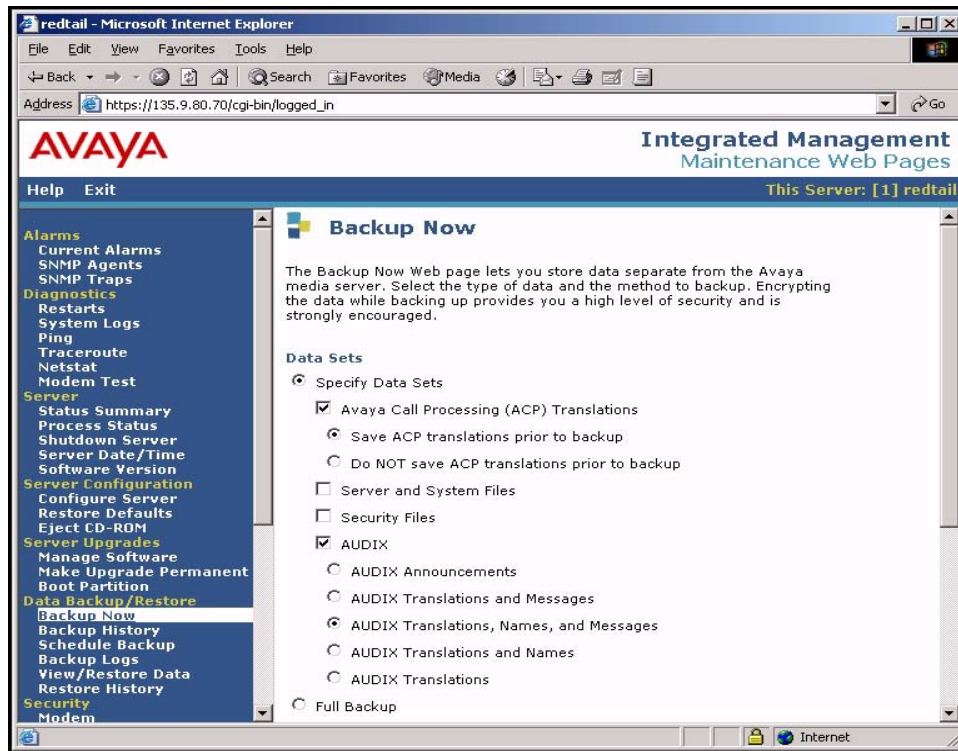
Before installing the S8300 software, back up the system data in case you need to back out of the upgrade. You should back up to an FTP, SFTP, or SCP server on the customer's network. To do this, you need an FTP, SFTP, or SCP address and directory path and a user ID and password to access the customer's network. Check with your project manager or the customer for this information. You can also back up the system data to the S8300 hard drive.

To back up S8300 recovery system data

1. Under Data Backup/Restore, click **Backup Now**.

The **Backup Now** screen displays.

Backup Now screen (Part One)



2. Select **Full Backup**, if available with the existing release, or select all data sets:

- Avaya Call Processing (ACP) Translations
- Save ACP translations prior to backup

Note:

Select ACP translations only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

- Server and System Files
- Security Files

3. If the AUDIX options are available, select AUDIX and select AUDIX Translations, Names, and Messages.



CAUTION:

Selecting the **Full Backup** radio button does *NOT* include AUDIX files. You must backup the IA770 INTUITY AUDIX data after you do the full backup.

Backup Now screen (Part Two)

AVAYA Integrated Management Maintenance Web Pages
This Server: [1] thehawk-icc

Help Exit

Alarms
Current Alarms
Agent Status
SNMP Agents
SNMP Traps
Filters
SNMP Test

Diagnostics
Restarts
System Logs
Ping
Traceroute
Netstat
Modem Test
Network Time Sync

Server
Status Summary
Process Status
Shutdown Server
Server Date/Time
Software Version

Server Configuration
Configure Server
Restore Defaults
Eject CD-ROM

Server Upgrades
Manage Software
Make Upgrade Permanent
Boot Partition

☐ Full Backup
Note: A CM "save trans" is not executed by the Full Backup

Backup Method

☐ Network Device

Method: SCP
User Name:
Password:
Host Name:
Directory:

☐ Local PC Card Retain: 9 data sets at destination
☐ Format PC Card

Encryption
☐ Encrypt backup using pass phrase:

Start Backup **Help**

4. Select **Network Device** and then select **FTP** for the backup method and fill in the appropriate fields with information provided by the customer.
5. Click **Start Backup** to back up the files.

Note:

The backup and restore processes use the ping service to check connectivity to the backup server. If a backup or restore operation fails, ensure that the ping service is enabled.

- i. On the Maintenance Web Interface, under **Security** select **Firewall**.
- ii. In the **Service** column, find **ping**.

The checkboxes for both **Input to Server** and **Output from Server** should be checked.

6. To check the status of the backup:
 - a. Under **Data Backup/Restore**, click **Backup History**.
 - b. Select the backup file and click **Check Status** to open the **Backup History Results** screen.

When the backup is finished, the **Backup History Results** screen displays

The final status for your backup job is shown below.

For each backup set, the message

BACKUP SUCCESSFUL

displays, if the set was backed up successfully.

7. If the AUDIX options are available, repeat Steps 3–6 for AUDIX Announcements.

Recording configuration information

If you have not already done so, you must record the current server configuration data, which will be re-entered after the upgrade.

To view and record the current configuration data

1. Launch the Maintenance Web Interface.
2. Under Server Configuration and Upgrades, click **Configure Server**.
3. Click **Continue** on the first and second screen.
4. On the **Select method for configuring server** screen, select **Configure individual services** and click **Continue**.
5. Select **Set Identities** from the left-side navigation pane and record the host name of the server.
6. Select **Configure Interfaces** and record the following:
 - Server IP address
 - Gateway IP address,
 - Subnet mask
 - Integrated Messaging IP address, if configured

You can skip the remaining configuration screens.

7. Select **Close window** and exit the Web pages.

Upgrade the S8300

Replacing the S8300B with the S8300C Media Server

To remove the S8300B and insert the S8300C

Note:

The G700 Media Gateway does *not* need to be powered down to perform this procedure.

1. On the Maintenance Web Interface, under Server select **Shutdown Server**.
2. Select the **Delayed Shutdown** option and *uncheck* the "Restart server after shutdown," checkbox.
3. Click the **Shutdown** button.
Click **OK** to confirm.
4. When the **OK to Remove** LED on the S8300 faceplate goes on steady, it is safe to remove the S8300 Media Server.



CAUTION:

Be sure to wear a properly grounded ESD wrist strap when handling the S8300 Media Server. Place all components on a grounded, static-free surface when working on them.

5. Loosen the two thumb screws on the S8300 faceplate.
6. When removing the S8300B Media Server, the LED module (above slot V1) must also be removed with the S8300 Media Server.
Disengage the LED module and the S8300 Media Server and remove them together from the G700.
7. If the IA770 INTUITY AUDIX module (CWY1 card) is installed on the S8300B Media Server, leave it on S8300B Media Server.

Note:

The CWY1 card is *not* supported on Communication Manager Release 4.0.

8. Reinsert the LED panel (above slot V1) until the front of the panel aligns with the front of the G700.

9. Connect the DVD/CD-ROM drive with the following steps:

Note:

You must do this *before* you completely seat the media server in the slot.

- a. Connect the USB cable into one of the USB ports on the faceplate of the S8300.
- b. Connect the other end of the USB cable to the CD-ROM or DVD/CD-RW drive.
- c. If you are using an Addonics DVD/CD-RW drive, connect the power cord to the drive and an electrical outlet.

Note:

The TEAC drive and S8300/S8400 DVD/CD-RW drive get their power from the server over the USB connection.

- d. If you are using the Addonics DVD drive, set the power source switch on the side to **EXT**, *not* **USB**.
- e. If you are using the S8300/S8400 DVD/CD-RW drive, set the on/off switch to **On**.

Be sure to set the S8300/S8400 drive to **Off** when not in use.

10. Insert the Communication Manager Software Distribution CD in the drive.



CAUTION:

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

Note:

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

11. Insert the S8300C circuit pack into the slot V1 guides until the front of the circuit pack aligns with the front of the G700.

When the server starts to boot, it looks for the software on the DVD/CD-ROM and continues to boot. The Alarm LED of the S8300 lights steadily as it is starting. The Alarm LED starts flashing when the S8300 is ready to load software.

12. Secure the S8300 faceplate with the thumb screws.

Tighten the thumb screws with a screw driver.

Note:

If the LED panel is not inserted all the way in, all of the status lights (on the left side of the LED panel) will be on. If this is the case, press the LED panel all the way in.

13. Reconnect the laptop to the services port of the new S8300C.

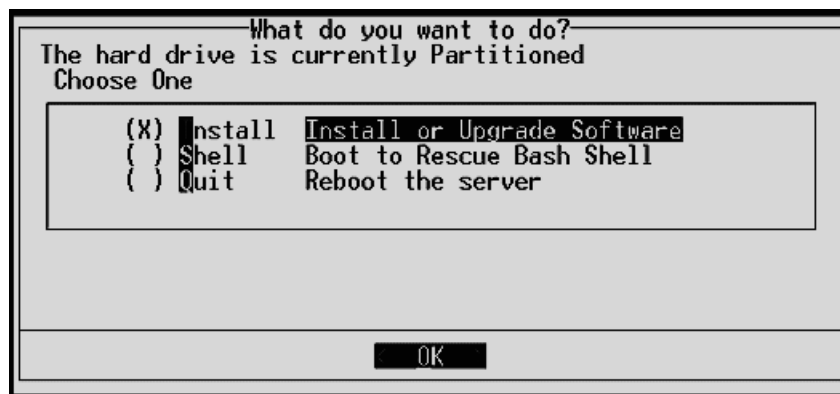
Remastering the hard drive and installing the software

To begin the upgrade

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.

The first RP screen appears.

The first RP screen



Tip:

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

Note:

At this point, the installation script looks for the software CD on the DVD/CD drive connected to the USB port. If the DVD/CD drive was not attached to a USB port when the S8300 booted, you will not see any activity on the screen. In this case, perform the following steps:

- Press the Shut Down button on the S8300 Media Server.
- When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port and reseal the S8300 in its slot.

3. Select **Install** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen



4. Select the appropriate release version (if more than one) then select **OK** and press **Enter**.
The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen



5. Select **Yes** if you want to install AUDIX concurrently with Communication Manager. Select **No** if you do not. Then press **Enter**.

Note:

If you do not install IA770 concurrently with Communication Manager at this time, and decide later to install it, you will have to upgrade Communication Manager again (even to the same release). For the upgrade, you use the Manage Software screen on the Maintenance Web interface, and select **Yes** at this screen for IA770 installation.

At this point, the following processes are initiated:

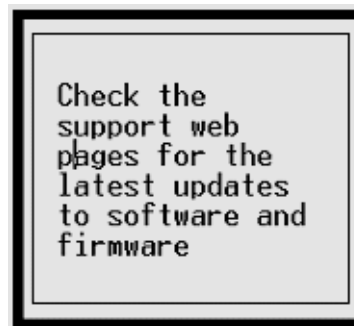
- a. The S8300 hard drive and internal Compact Flash drive are partitioned and reformatted.
- b. The Linux operating system is installed.
- c. The program begins installing Communication Manager software and reports the progress.

Communication Manager installation progress

```
21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.69-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktmp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popd-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm
```

These processes take about 30 minutes. When the media server is ready to reboot, the CD drive door opens and the following screen flashes for about 5 seconds.

Software and firmware update reminder



When the installation is complete, the system reboots automatically and the telnet connection is lost. The reboot takes 1–3 minutes without the IA770 application and 3-6 minutes if the IA770 is present.

6. Click **Start > Run** to open the **Run** dialog box on your laptop.
7. Type `ping -t 192.11.13.6` and press **Enter**.
8. Wait for the reply.

Verifying Software Version

Note:

Since the system is now running a new software release, you must login with the *initial craft ID and password*. (You cannot use *dadmin* at this point.)

To verify the software version:

1. Log in to the Maintenance Web Interface.

See [Logging in to the S8300 Web Interface from your laptop](#) on page 57.

2. Under Server, click **Software Version**.
3. Verify that the media server is running Release 4.0 software.

The **Report as:** string should show **R014x.00** at the beginning of the string. For example, **R014x.00.0.728.0**.

4. Verify that the DVD/CD-ROM drive popped open and disconnect the DVD/CD-ROM drive from the S8300 USB port.

Copying Files to the S8300 hard drive

During reformatting of the hard drive, a new directory, */var/home/ftp/pub*, was created.

You must copy the remaining required files to the *pub* directory on the S8300 hard drive. This includes, but is not limited to:

- Post-upgrade software service pack
- License file
- Avaya authentication file
- New firmware files
- Security updates
- IA770 service packs or RFUs

To copy files to the S8300 hard drive

1. Under **Miscellaneous** on the Maintenance Web pages, click **Download Files**.

Download Files screen

Download Files

The Download Files Web page lets you download files to the media server.

☒ File(s) to download from the machine I'm using to connect to the server

☐ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

☐ Install this file on the local server

**If the above box is checked, you may specify only one file for downloading.

2. Select "Files to download from the machine I'm using to connect to the server" and browse to each file you want to copy to the S8300. Leave the "Install this file on the local server" checkbox **unchecked**.

If you need to download an IP Telephone firmware file, download this file last with the "Install this file on the local server" checkbox **checked**.

Note:

To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to `pub` after starting ftp and logging in; that is, type `cd pub`.

3. Click on **Download** to copy the files to the S8300. The transfer is complete when you see the message,

Files have been successfully uploaded to the server



Important:

Remove the Communication Manager software distribution CD from the DVD/CD-ROM drive.

Downloading optional language files, if needed

If the optional language files are needed, copy the files from the language CD to `/var/home/ftp/pub`.

To download optional language files

1. Insert the optional language CD in your laptop's CD-ROM drive.
2. On the Maintenance Web Interface, under Miscellaneous, select **Download Files**.
3. Select the **Files to download from the machine I'm using to connect to the server** download method.
4. Browse to the laptop CD and select each language file that you wish to copy.
5. Click the **Download** button.

When the transfer is complete, the message

Files have been successfully downloaded to the server

is displayed.

6. If more than four optional language files need to be downloaded, repeat this procedure.

Copies of the optional language files are now in the `/var/home/ftp/pub` directory and will be automatically installed during the upgrade process.

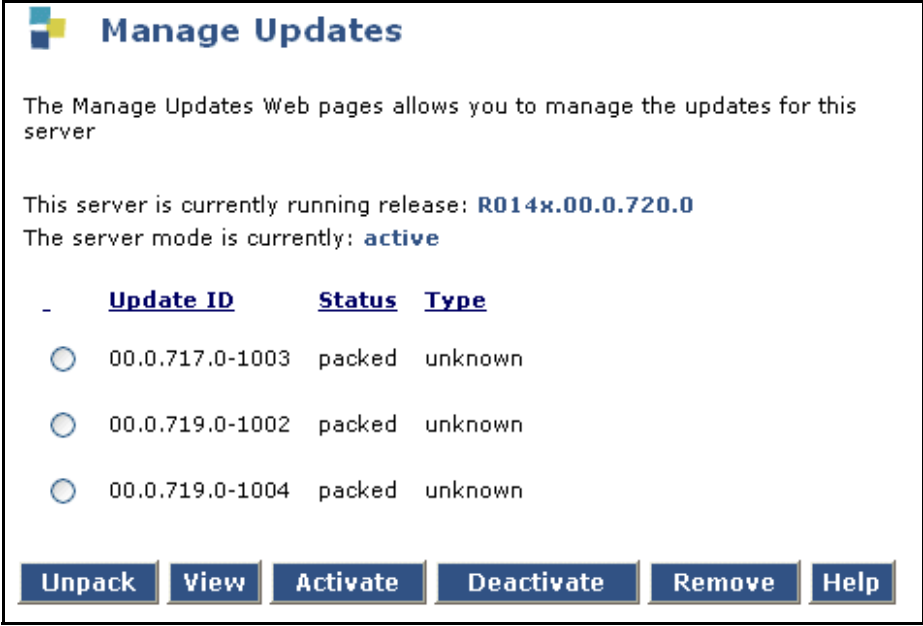
Installing security and Communication Manager service pack updates, if any

To install update files

1. Under Server Upgrades, select **Manage Updates**.

The **Manage Updates** screen appears.

Manage Updates Screen



Manage Updates

The Manage Updates Web pages allows you to manage the updates for this server

This server is currently running release: **R014x.00.0.720.0**
The server mode is currently: **active**

	<u>Update ID</u>	<u>Status</u>	<u>Type</u>
☐	00.0.717.0-1003	packed	unknown
☐	00.0.719.0-1002	packed	unknown
☐	00.0.719.0-1004	packed	unknown

Unpack View Activate Deactivate Remove Help

2. If an update file you want to activate shows **packed** in the **Status** column, select update ID and click **Unpack**.

The window shows the status of the unpacking.

3. Wait until the system displays the message **Finished unpacking...** and click **Continue**.

The system displays the **Manage Updates** screen.

4. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.

The screen shows the status of activating the update. If a reboot is required, the system automatically reboots.

5. Click **Yes**.

Wait until the system displays the Continue button.

6. Click **Continue**.

Setting the Time, Date, and Time Zone

To set the Time, Date, and Time Zone:

1. Under Server click **Server Date/Time**.

Server Date/Time Window

Server Date/Time

The Server Date/Time Web page lets you reset date and time when the server is used as its own time source.

The current time is: **Wed Aug 20 19:10:00 MDT 2003**

Date (mm/dd/yyyy)

Select time (hh:mm)
Use 24-hour format

Time Zone

- America/Denver
- America/Detroit
- America/Dominica
- America/Edmonton
- America/Eirunepe
- America/El_Salvador
- America/Ensenada
- America/Fort_Wayne

2. Set the media server's time close enough to the Network Time Server's (NTS's) time, date, and time zone that synchronization can occur (within about 5 minutes).

! CAUTION:

If you are installing an LSP, you must set the time of the LSP to the same time zone as the primary controller even if the LSP is physically located in a different time zone.

Configuring network parameters

Note:

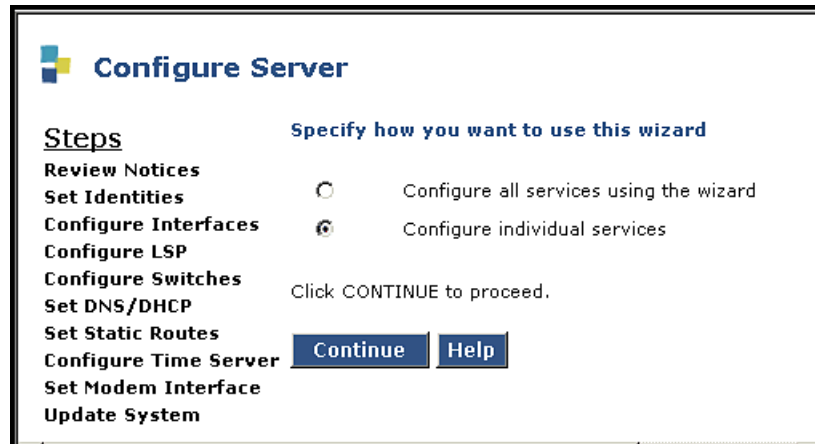
For this procedure, you must have the host name, subnet mask, and IP address of the S8300, and the IP address of the default gateway.

You must configure the network parameters on the S8300 before restoring the backup files. These network parameters are necessary to allow the media server to reach the FTP backup server over the network.

To configure network parameters

1. Under Server Configuration click **Configure Server** to start the configure server process.
2. Click **Continue** through the **Review and Backup Notices** to get to the **Specify how you want to use this wizard** screen.

Specify how you want to use this wizard screen



3. Select **Configure individual services** and click **Continue**.
4. Click **Set Identities** from the "Configure Individual IP Services" list on the left.
The **Set Identities** screen appears.
5. Fill in the Host name screen with the name of the server.
6. Click **Continue**.
The **Configure Ethernet Interfaces** screen displays.

Configure Ethernet Interfaces screen (primary controller example)

Configure Server

Configure Interfaces

Ethernet 0: Laptop
 IP address 192.11.13.6
 Subnet mask 255.255.255.252

Ethernet 1: Control Network
 IP address server1 (swainsons-icc) 135.9.127.60
 Gateway 135.9.127.254
 Subnet mask 255.255.255.0
 Speed (Current speed : 100 Megabit full duplex) AUTO SENSE

Integrated Messaging
 IP address server1 (swainsons-icc)

Click **CHANGE** to change values.

Change **Close Window** **Help**

Local intranet

- Fill in the correct server IP address, Gateway, Subnet mask, and, if IA770 was installed, the Integrated Messaging IP address. The Integrated Messaging IP address is not available with an LSP.

If these fields are already filled in, overwrite them with the correct information. Leave the Integrated Messaging field blank.

Click **Change** to update the system files.

Note:

If an **Action Cancelled** message appears before the success message, refresh the screen and click **Change** again.

- When the configuration change is complete, the screen displays **Successfully configured ethernet interfaces**. Click **Close Window**.

At this point, the system resets the IP interfaces.

Verifying connectivity

To verify that the Ethernet port is working, ping the FTP server where the backup file(s) are stored.

To verify connectivity

1. On the Maintenance Web Interface, under Diagnostics click **Ping**.
2. Enter the IP address where the backup files are stored.
3. Click **Execute Ping**.

If the ping is successful, continue with restoring the system files. Otherwise, check the IP address and connectivity to the server.

Disabling RAM disk on the media server

You must disable RAM disk prior to restoring the S8300 configuration data. To disable RAM disk, perform the following steps:

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. At the command line, type `sudo ramdisk -v -f disabled`, and press **Enter**.
The system does not display any information to the screen if there are no errors.
3. At the command line, type `ramdisk -v -s` and press **Enter**.

Rebooting the media server

To reboot the media server, perform the following steps:



CAUTION:

Be sure the DVD/CD-ROM drive is not connected.

1. On the Maintenance Web Interface, under Server select **Shutdown Server**.
2. Select the **Delayed Shutdown** option. Also, be sure the **Restart server after shutdown** checkbox is selected.
3. Click the **Shutdown** button.
Click **OK** to confirm.
4. At the command line, type `ramdisk -v -s` and press **Enter**.
Confirm that the system has disabled RAM disk.

Restoring all data

To restore all data to the media server, do the following:

1. On the Maintenance Web Interface, under Data Backup/Restore select **View/Restore Data**.

The system displays the **View/Restore Data** screen.

View/Restore Data screen

2. Select **FTP**.

Fill in the **User Name**, **Password**, **Host Name (enter host IP Address)**, and **Directory** fields for the location of the backup file on the customer's server.

3. Click **View**.

The system displays the **View/Restore Data Results** screen.

View/Restore Data Results screen

View/Restore Data Results

List of backup images (x.tar.gz) at specific location:

File Name
☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_092458_20031121.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_094952_20040420.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_125559_20040502.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/os_doc-icc1_162851_20040428.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_092507_20031121.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_095003_20040420.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_125611_20040502.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/security_doc-icc1_162903_20040428.tar.gz
☒ /usr/add-on/systest/translations/doc-icc1/upgrade-2.0_doc-icc1_105127_20030909.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/upgrade-2.0_doc-icc1_160417_20030908.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_092435_20031121.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_094933_20040420.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_125534_20040502.tar.gz
☐ /usr/add-on/systest/translations/doc-icc1/xln_doc-icc1_162828_20040428.tar.gz

Pass Phrase:

☐ Force restore if server name mismatch.
☐ Force restore if backup version mismatch.

Restore **Preview** **Help**

4. Select the backup file with the name starting with "os" or select the full backup with the name starting with "full." The full backup contains the system, security, and translations backup data. It does *not* include IA770 INTUITY AUDIX data.

Note:

The time and date are embedded in the file name. Select the backup set with the current time and date stamp.

5. Select both **Force** options, and click **Restore**.

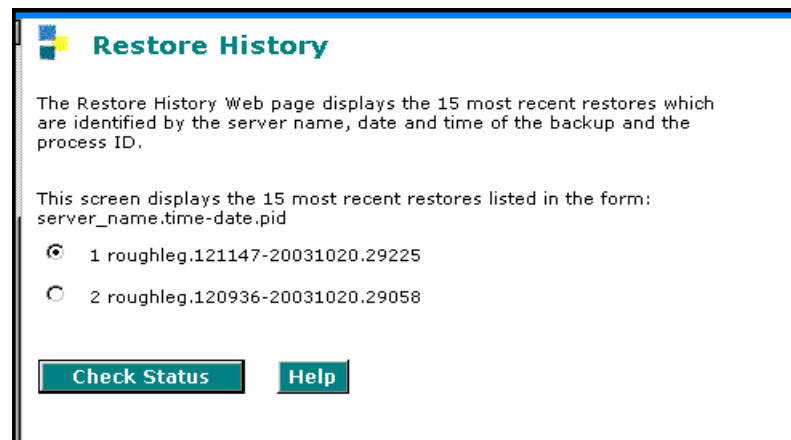
The View/Restore Data Results page appears

6. To monitor the restore progress:

- a. Click **Check status**.

The **Status** screen displays.

Restore History screen



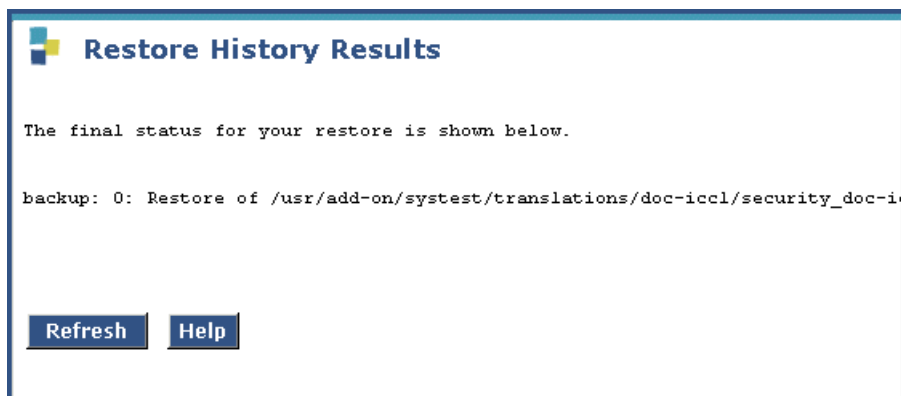
- b. Select the backup set being restored and click **Check Status**.

The **Restore History Results** screen displays.

- c. Click **Refresh** periodically until the message,

The final status for your restore is shown below appears.

Restore History Results screen



7. Repeat the restore procedure for the remaining backup sets in the following order:

Note:

If you restored a full backup, you do not need to restore the security and translations data backups.

- Security data in the file whose name begins with "security."
- (For a primary controller only, not an LSP) Translations data in the file whose name begins with "xln."
- (For a primary controller only, not an LSP) INTUITY AUDIX data in the file whose name begins with "audix-tr-name-msg."
- INTUITY AUDIX data in the file whose name begins with "audix-ann".

Checking for the IA770 IP address

1. Under Server Configuration click **Configure Server** to start the configure server process.
2. Click **Continue** through the **Review and Backup Notices** to get to the **Specify how you want to use this wizard** screen.
3. Click **Configure Interfaces** from the “Configure Individual IP Services” list on the left.

The **Configure Interfaces** screen displays.

Configure Interfaces screen (primary controller example)

Configure Server

Configure Interfaces

Ethernet 0: Laptop

IP address	192.11.13.6
Subnet mask	255.255.255.252

Ethernet 1: Control Network

IP address server1 (swainsons-icc)	135.9.127.60
Gateway	135.9.127.254
Subnet mask	255.255.255.0
Speed (Current speed : 100 Megabit full duplex)	AUTO SENSE

Integrated Messaging

IP address server1 (swainsons-icc)	

Click **CHANGE** to change values.

Change **Close Window** **Help**

Local intranet

4. Check that the Integrated Messaging IP address is available.
5. If the IP address is available, click Close Window.
6. If the IP address is not available, enter the IP address and click Change.

Note:

If an **Action Cancelled** message appears before the success message, refresh the screen and click **Change** again.

When the configuration change is complete, the screen displays **Successfully configured ethernet interfaces**. Click **Close Window**.

At this point, the system resets the IP interfaces.

Enabling RAM disk on the media server

To enable RAM disk, perform the following steps:

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. At the command line, type `sudo ramdisk -v -f enabled`, and press **Enter**.
3. At the command line, type `ramdisk -v -s` and press **Enter**.

Rebooting the media server

To reboot the media server, perform the following steps:

1. On the Maintenance Web Interface, under Server select **Shutdown Server**.
2. Select the **Delayed Shutdown** option. Also, be sure the **Restart server after shutdown** checkbox is selected.
3. Click the **Shutdown** button.

Click **OK** to confirm.

4. At the command line, type `ramdisk -v -s` and press **Enter**.

Confirm that the system has enabled RAM disk.

Note:

It is good practice to close the browser after the reboot and log back in.

Installing updated license and authentication files



CAUTION:

A super-user login, dadmin or another customer superuser login, must exist *before* you install an authentication file. If the authentication file does not install, you might need to create a super-user login, then install the new authentication file. See [Checking a 4.0 release for a super-user login](#) on page 731.

To install the license and authentication files:

1. On the Maintenance Web Interface menu under Security, select **License File**.

The **License File** screen displays.

License File Screen

License File

The License File Web page allows installation of Avaya license files.

CommunicationsMgr License Mode: Normal
Network used for License: Carrier MGP
License Serial Number is 01DR12310260 on carrier MGP

☐ Undo last install
☒ Install the license file I previously downloaded
☐ Install the license file specified below

File Path
URL
Proxy Server e.g proxy.domain:3152

2. Select **Install the license file I previously downloaded** and click **Submit**.

The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.
4. The **Authentication File** screen displays.

Authentication File screen

Authentication File

The Authentication File Web page allows installation of Avaya authentication files.

☒ Install the Authentication file I previously downloaded
☐ Install the Authentication file I specified below

File Path

URL

Proxy Server (e.g. proxy.domain:3152)

5. Select **Install the Authentication file I previously downloaded** and click **Install**.

The system tells you the authentication file is installed successfully.

Checking a 4.0 release for a super-user login

To ensure that a super-user login exists in Communication Manager in Release 4.0 or higher:

1. Log in with **ssh**.
2. At the Linux command line, type **cat /etc/passwd | grep 555**.

The following list of super-user logins appears.

```
init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1001:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash
```

3. Look for any logins other than the init, inads, and craft logins. If no additional super-user logins exist, you must create one. See [Creating a super-user login, if necessary, for R4.0 or higher](#).

Creating a super-user login, if necessary, for R4.0 or higher

If a super-user login does not exist, you must add at least one before you complete the upgrade. The easiest way to add a login is with the Maintenance Web pages. Use the following steps only if you are starting from Release 4.0 software or later:

Note:

A craft level login can create a super-user login in Release 4.0 or later.

Note:

If you are installing software for an S8300 LSP, create the super-user login on the primary controller. Then, at the Linux command line on the primary controller, run the `filesync -a <IP_address_of_LSP>` command.

To create a login:

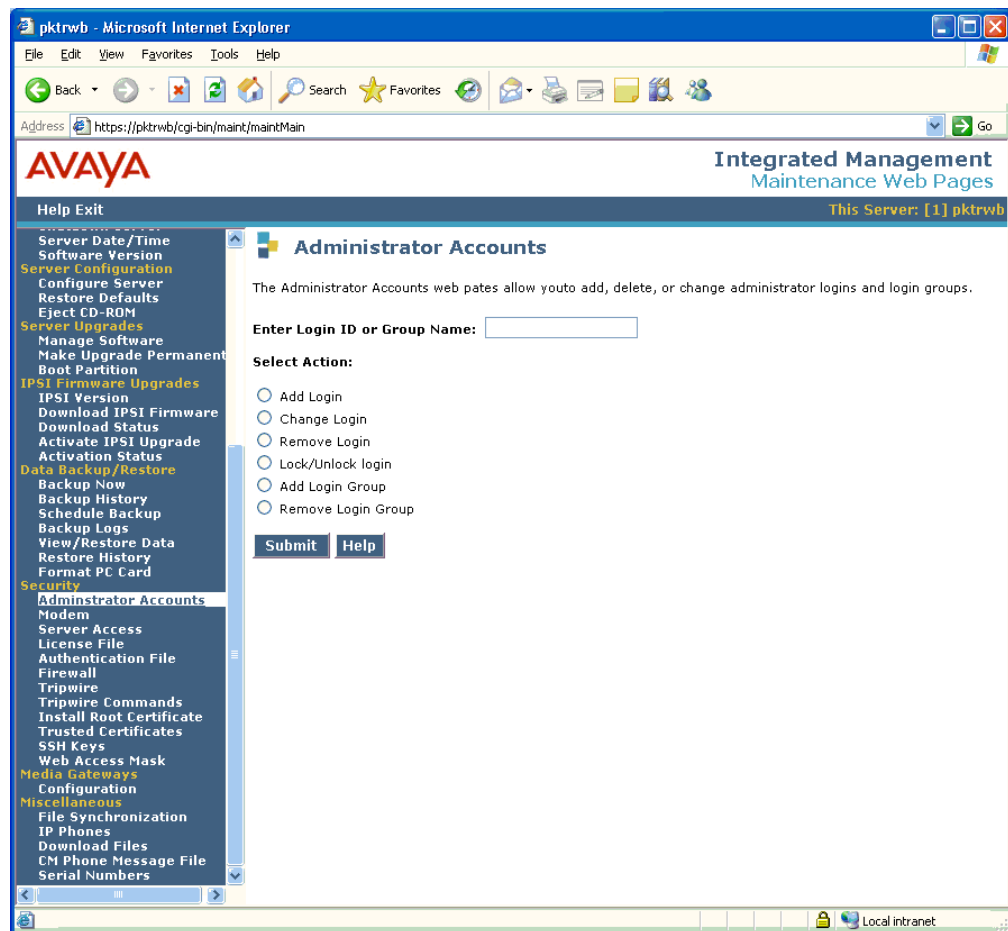
1. Ask a customer representative for a login name and password that the customer would like for the superuser login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Note:

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

2. Under **Security**, select **Administrator Accounts**.

The **Administrator Accounts** screen appears.



3. Type the login name in the **Enter Login ID or Group Name** field.

4. Select **Add Login**, and click **Submit**.

The Administrator Logins -- Add Login screen appears.

The screenshot displays the Avaya Integrated Management Maintenance Web Pages interface. The top header shows the Avaya logo and the title 'Integrated Management Maintenance Web Pages'. Below the header, a navigation menu on the left lists various system management tasks, including 'Restore Defaults', 'Server Upgrades', 'IPSI Firmware Upgrades', 'Data Backup/Restore', and 'Security'. The 'Security' section is expanded, showing 'Administrator Accounts' as the selected option. The main content area is titled 'The Administrator Logins -- Add login web page allows you to add a new administrator login.' and contains the following fields and options:

- Login ID:** Pre-filled with 'randy'.
- login group:** Text field containing 'susers'.
- additional groups:** Text field containing 'prof18'.
- allow Linux shell access:** Radio button, currently unchecked.
- lock this account:** Radio button, currently unchecked.
- date (YYYY-MM-DD) on which account is disabled (blank to ignore):** Empty text field.
- select type of authentication:** Radio buttons for 'password' (selected) and 'ASG'.
- enter key or password:** Empty text field.
- re-enter key or password:** Empty text field.
- force password/key change on first login:** Radio buttons for 'yes' and 'no' (selected).
- maximum Number of days a password may be used (PASS_MAX_DAYS):** Text field containing '90'.
- minimum number of days allowed between password changes (PASS_MIN_DAYS):** Text field containing '90'.
- minimum acceptable password length (PASS_MIN_LEN):** Text field containing '8'.
- number of days warning given before a password expires (PASS_WARN_AGE):** Empty text field.
- days after password expires to lock account (0=immediate):** Empty text field.

At the bottom of the form are 'Add' and 'Help' buttons. The status bar at the very bottom shows 'Done' and 'Internet' connectivity.

5. Type **susers** in the **login group** field.
6. Type **prof18** in the **additional groups** field. *prof18* is the code for the customer superuser.
7. Put a check in the **allow Linux shell access** field.
8. Skip the **lock this account** and **date on which account is disabled** fields.
9. For the **select type of authentication** option, select **password**.

10. Complete the following fields:

- enter a challenge key or password
- re-enter challenge key or password
- force password/key change on first login

Note:

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

11. Leave the defaults in the remaining fields.

12. Click **Add**.

The system tells the login is added successfully.

13. If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

- a. Log in with `telnet` or `ssh`.
- b. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If upgrading an LSP, synchronize translations from the primary controller

If you are upgrading an LSP such that you created this super-user login on the primary controller, do the following also on the primary controller.

1. Log in with `telnet` or `ssh`.
2. At the Linux command line, type `filesync -a <IP_address_of_LSP>`, where `<IP_address_of_LSP>` is the IP address of the LSP you are upgrading.

If the server is an LSP, stop and start Communication Manager

If you are upgrading an LSP, you must restart Communication Manager to sync the license for LSP status.

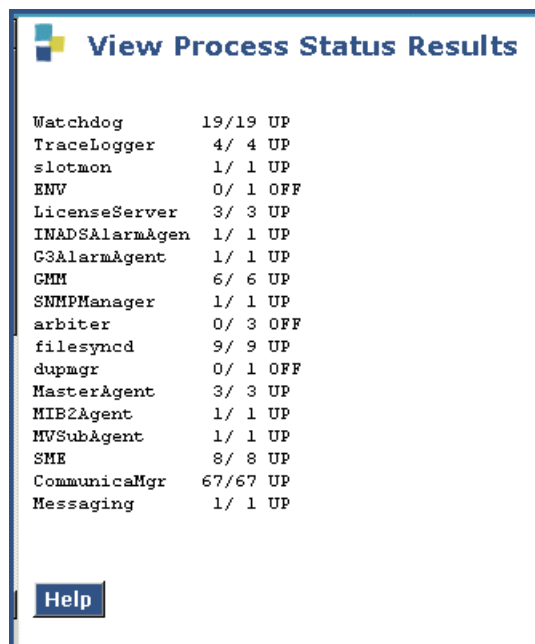
1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `stop -caf`
3. Type `start -ca`

If IA770 INTUITY AUDIX Messaging has been upgraded, verify messaging has started

If you installed IA770 INTUITY AUDIX Messaging, the messaging application should start after you install the license. To verify that messaging has started, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.
the **View Process Status Results** screen displays.

View Process Status screen



Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

[Help](#)

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

If you need to start messaging, you can use either the Maintenance Web pages or the Linux command line. For the Maintenance Web pages, see [Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary](#) on page 737. For the Linux command line method, see [Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary](#) on page 737.

Starting IA770 INTUITY AUDIX Messaging with the Messaging Web pages, if necessary

1. From the Maintenance Web Page, select **Messaging Administration** from the **Miscellaneous** menu.

The Messaging Administration Web page is displayed in a new Web browser window.

2. From the Messaging Administration Web page, select **Utilities**.

The Utilities Web page is displayed.

3. Select **Start Messaging Software**.

The Start Messaging Software Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

Starting IA770 INTUITY AUDIX Messaging with the command line, if necessary

1. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
2. Type `start -s Audix`

3. Ensure that all Communication Manager processes come up.

To monitor the startup of IA770:

- a. Type `watch /VM/bin/ss`

The display will periodically refresh automatically. When you see the following display, the IA770 startup is complete.

- b. Press **Ctrl+C** to break out of the `watch` command.

If IA 770 fails to start after an upgrade

If you have upgraded your Communication Manager and IA 770 INTUITY AUDIX software, you must have a new license that is associated with the latest release. IA 770 will not use the license for a previous version.

If you upgraded IA 770 without a new license file, it will fail to start during the Communication Manager startup sequence.

If this occurs, you must do the following steps:

1. Obtain an IA 770 Replace variable w/ release number license file.
2. Install the license file.
3. From a command prompt, start the IA 770 process with the following command:

```
start -s Audix
```

Saving translations

Note:

If the S8300 you are upgrading is an **LSP**, perform this task on the primary controller.

To save translations

1. In the SSH session, open a SAT session. and log in as *craft* (or *dadmin*).
2. If the S8300 you are upgrading is a primary controller, at the SAT prompt, type `save translation` and press **Enter**.

3. If the S8300 you are upgrading is an LSP, then on the primary controller, type **save translation lsp** and press **Enter**. This command distribute saved translations out to the LSPs.

When the save is finished, the system displays the message,

Command successfully completed.

The system automatically performs a reset system 4. If you are upgrading an LSP, you are logged out.

Copying IP Phone firmware to the media server, if necessary

If, before the upgrade, the server was serving as an http server for IP phone firmware, download the most recent IP phone firmware bundle available from the Avaya Firmware Download Web site. The firmware bundle reinstates the 46xx IP Phone Web page in Communication Manager and also makes the 46xx IP Phone firmware for the tftp or http server capability of the media server.

Note:

The IP phone firmware that was originally downloaded will have been overwritten.

To copy files to the media server:

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

The files are copied automatically to the /tftpboot directory. The 46xx IP Phone Web page is reinstated at the next reboot.

Restoring the 4600-series phone configuration file, if any

If you copied a 4600-series phone configuration file to the **/var/home/ftp/pub** directory prior to the upgrade, the customer should use ftp to restore the file to /var/home/ftp/pub. You should then restore it to the /tftpboot directory. However, before you restore the file, be sure you have downloaded the appropriate IP phone firmware.

1. At the Linux command line, type `cd ~ftp/pub`, and press **Enter**.
2. At the prompt, type `cp 46xxsettings.txt /tftpboot`, and press **Enter**.

The 4600-series phone settings file is now restored to the /tftpboot directory.

Upgrade the G700 firmware

This section describes how to upgrade firmware on the components of the G700, including the Media Gateway Processor (MGP), the P330 Stack Processor, and any installed media modules. Alternate methods to upgrade the G700 Media Gateway include using the Avaya Installation Wizard, the Upgrade Tool, or Software Update Manager.

Verifying the contents of the tftpboot directory

Before proceeding with the G700 firmware installation, you should check the */tftpboot* directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the */tftpboot* directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.



CAUTION:

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the */var/home/ftp/pub* directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the *pub* directory.

3. Copy the firmware files from the *pub* directory to the */tftpboot* directory, using the S8300 Media Server command line interface.

To copy firmware files to the */tftpboot* directory of an S8300 Media Server, do the following:

- a. Access the server's command line interface using an SSH client, like PuTTY, and an IP address of **192.11.13.6**.
- b. Log in as *craft*.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to */var/home/ftp/pub*.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the */tftpboot* directory. To copy multiple firmware files (most firmware files have an *.fdl* suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the */tftpboot* directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to */tftpboot*.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

Conduct the following procedure to compare software versions running on the G700 processors and media modules with the versions in you planning documents. If the versions do not match, you need to install the new firmware for those components.

To determine if new firmware for the P330 stack processor is necessary

1. Access the stack processor. See one of the following:
 - [Logging in to the P330 Stack Processor with a Direct Connection to the S8300 Services Port](#) on page 62
 - [Logging in to the P330 Stack Processor with a LAN Connection](#) on page 63
 - [Logging in to the P330 Stack Processor with a Direct Serial Connection](#) on page 64
 - [Logging in to the P330 Stack Processor with Device Manager](#) on page 64
2. At either the **P330-1(super)#** or **P330-1(configure)#** prompt, type `dir`.

The system displays the directory list of software for the P330 stack processor.

Directory list for P300 stack processor

M#	file	ver num	file type	file location	file description
--	----	-----	-----	-----	-----
1	module-config Configuration	N/A	Running Conf	Ram	Module
1	stack-config	N/A	Running Conf	Ram	Stack Configuration
1	EW_Archive	4.0.4	SW Web Image	NV-Ram	WEB Download
1	Booter_Image	3.2.5	SW BootImage	NV-Ram	Booter Image

3. Check the version number (ver num) of the EW_Archive file to see if it matches the Release Letter.

If not, you must upgrade the P330 stack processor.

4. Type **show image version**

The system displays the list of software.

Show image version List for P330 stack processor

Mod	Module-Type	Bank	Version
-----	-----	----	-----
3	Avaya G700 media gateway	A	0.0.0
3	Avaya G700 media gateway	B	4.0.17

5. Check the version number of the stack software image file in Band B to see if it matches the your planning document.

If not, you must upgrade the P330 stack processor.

To determine if new firmware is required for the MGP, VoIP module, and installed media modules

1. Type **session mgp**
2. At the **MG-001-1(super)#** prompt, type **show mg list_config**

The system displays the list of software.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (B)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

3. Refer to the list to check the FW vintage number of the G700.

In the TYPE column, find G700, then check the matching field in the FW VINTAGE column to see if it matches the vintage number in your planning forms. If not, you must install new firmware on the G700 media gateway. Also check if the release number in the FW VINTAGE column contains (A) or (B) to designate the software bank. If the list shows B, you will upgrade A. If the list shows A, you will upgrade B.

4. Refer to the VOIP FW column and row for slot V0 (same row occupied by the G700 information) to see if the number matches the VoIP firmware identified in your planning forms.

If not, you must also upgrade the G700 media gateway motherboard VoIP module.

Note:

The VoIP processor on the motherboard is upgraded using the same firmware image file as the VoIP media modules; for example, the file mm760v8.fdl is vintage #8.

5. Check the FW VINTAGE column for vintages of each of the installed media modules: MM710, MM711, MM712, MM720, and/or MM760 to see if they match the FW vintages in the planning forms.

If not, you must upgrade them, as well.

Installing new firmware on the P330 stack processor

To Install P330 stack processor firmware

1. From your S8300 telnet session, telnet back to the P330 stack processor:

Type `telnet <xxx.xxx.xxx.xxx>`,

where `<xxx.xxx.xxx.xxx>` is the IP address of the P330 stack master processor on the customer's LAN.

2. At the **P330-1(configure)#** prompt, type

```
copy tftp SW_image <file> EW_archive <ew_file>
<tftp_server_address> <Module#>
```

where `<file>` is the full-path name for the image file with format and vintage number similar to viisa3_8_2.exe,

`<ew_file>` is the full-path name for the embedded web application file with format similar to p330Tweb.3.8.6.exe,

`<tftp_server_ip_address>` is the IP address of the TFTP server, and

`<Module#>` is the number, 1 through 10, of the media gateway in the stack. If there is only one G700 media gateway, the number is 1.

3. Verify that the download was successful when the prompt returns:
 - a. type `show image version <module #>` and check the version number in the Version column for Bank B.
 - b. type `dir <module #>` and check the version number in the ver num column for the EW_Archive file.
4. Type `reset <module #>`.

Installing new firmware on the G700 Media Gateway Processor

To install MGP firmware

1. At the **P330-1(configure)#** prompt, type `session mgp` to reach the G700 media gateway processor.
2. Type `configure` at the **MG-???-1(super)#** prompt to enter configuration mode, which will change the prompt to **MG-???-1(configure)#**.
3. At the **MG-???-1(configure)#** prompt, type `show mgp bootimage` to determine which disk partition (bank) is in the **Active Now** column.

You will update the bank that is *not* listed as Active Now. The system displays the following screen:

Example: Show mgp bootimage

<u>FLASH MEMORY</u>	<u>IMAGE VERSION</u>
Bank A	109
Bank B	210
<u>ACTIVE NOW</u>	<u>ACTIVE AFTER REBOOT</u>
Bank B	Bank B

4. At the **MG-???-1(configure)#** prompt, type


```
copy tftp mgp-image <bank> <filename> <tftp_server_ip_address>
```

 to transfer the mgp image from the tftp server to the G700,
 where
 - <bank>** is the bank that is *not* Active Now (Bank A in the example).
 - <filename>** is the full path name of the mgp firmware image file, which begins with mgp and will be similar to the name mgp_8_0.bin.
 - <tftp_server_ip_address>** is the IP address of the S8300.
 For example:


```
copy tftp mgp-image a mgp_8_0.bin 195.123.49.54
```

 The screen shows the progress.

5. Type `set mgp bootimage <bank>`

where *<bank>* is the same letter you entered in the previous step.

6. At the **MG-???-1(configure)#** prompt, type `reset mgp`.

A system prompt asks you to confirm the reset.

7. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

8. When the **P330-1(super)#** prompt appears, type `session mgp`.

9. At the **MGP-???-1(super)#** prompt, type `configure`.

10. Verify that the download was successful when the prompt returns.

Type `show mg list_config`.

The system displays the list of software.

Example: Show mg list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	230 (A)	67
V1	ICC	S8300	A	72	00	N/A
V2	DCP	MM712	A	2	58	N/A
V3	ANA	MM711	A	2	57	N/A
V4	DS1	MM710	A	1	58	N/A

Installing new firmware on the media modules

For upgrades of active media modules, you need to take the media modules out of service before initiating the upgrade process. To do this, go to a SAT session on the primary controller and issue a `busyout` command.

Note:

Skip this busyout procedure if the media modules are not in service; for example during an initial installation.

To busyout board (for active media modules)

1. Go to a SAT session on the primary controller and enter the command,

`busyout board vx`

where *x* is the slot number of the media module to be upgraded.

2. Verify the response,

Command Successfully Completed

3. Repeat for each media module to be upgraded.

To install media module firmware

1. Be sure that you have checked for the current vintage of the VoIP Module for the v0 slot (on the G700 motherboard).

This VoIP module does not occupy a physical position like other media modules.

2. At the **P330-1(configure)#** prompt, type **session mgp**.
3. At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.
4. Type **copy tftp mm-image v<slot #> <filename mm> <tftp_server_ip_address>**

where

<slot #> is the slot of the specific media module,

<filename mm> the full-path name of the media module firmware file in a format such as mm712v58.fdl, and

<tftp_server_ip_address> is the ip address of the S8300.

Two or three minutes will be required for most upgrades. The VoIP media module upgrade takes approximately 5 minutes. Screen messages indicate when the transfer is complete.

5. After you have upgraded all the media modules, verify that the new versions are present.

At the **MG-???-1(configure)#** prompt, type **show mg list_config**

The list of software appears.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (A)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

6. In the **TYPE** column, find the particular media module (v1 through v4), then check the matching field in the **FW VINTAGE** column to see if it matches the planning documentation.

Note:

Slot V1 can contain either a media module or the S8300, which will show as
TYPE ICC.

7. Check the **VOIP FW** column and row for slot v0 to see if the number matches the VoIP firmware identified in the planning documentation.
8. Type **reset <module #>**
where **<module #>** is the number of the G700 in the stack.
9. When the reset is finished, type **show mm** to verify the upgrade.

To release board (if media module was busied out)

1. When the upgrade procedure is complete, go to the SAT session and release the board

Type **release board vx**

where **x** is the slot number of the upgraded media module.

2. Verify the response,

Command Successfully Completed

Note:

If you see the response, Board Not Inserted, this means that the media module is still rebooting. Wait one minute and repeat the **release board** command.

3. Repeat the **release board** command for each media module that was busied out.

Ensuring the MGP default gateway IP address is set

Communication Manager release 4.0 requires that the built-in VoIP module of the G700 Media Gateway has a default gateway IP address. To ensure that this IP address is set, perform the following steps:

1. At the **MG-???-1(configure)#** prompt, type **show ip route mgp**.

The list of mgp routes appears.

MG-001-1(super)# show ip route mgp				
DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	135.9.80.254	motfec0	(3/0/165)
135.9.80.0	255.255.255.0	135.9.80.88	motfec0	(101/0/0)
MG-001-1(super)#				

2. Check that a Gateway IP address exists for Destination 0.0.0.0.

3. If a Gateway IP address does not exist, type, at the **MG-???-1(configure)#** prompt, **set ip route 0.0.0.0 0.0.0.0 <IP_address>**, where **<IP_address>** is the default gateway IP address.

After you reboot the media gateway, the IP address is active and available.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 stack processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* (available at <http://www.avaya.com/support>).

Installing new firmware on other G700 media gateways

Installing G700 firmware in a stack configuration

If the customer has multiple G700 media gateways connected in an IP stack, you can stay connected to the master G700/P330 and "session" over from the master P330 Stack Processor to the next G700 in the stack. If you are dialed in remotely, you should have automatically dialed in to the stack master. For a local installation, you should have plugged your laptop into the stack master P330, which you can identify by the LED panel on the upper left of each G700 or P330 device in the stack.

The LEDs signal as follows:

- On the G700 Media Gateway: a lit **MSTR** LED indicates that this unit is the stack master.
- On the P330 device: a lit **SYS** LED indicates that this unit is the stack master.

The G700 and P330 at the bottom of the stack is module number 1, the next module up is number 2, and so on. However, the stack master can be any module in the stack, depending on the actual model, the vintage firmware it runs, and whether the S8300 is inserted into it.

Note:

You do not need to configure the other P330 processors in the stack. These will use the IP address and IP route of the master stack processor. However, you will need to check firmware on all devices of the other G700s in the stack, including the media gateways themselves, and update the firmware as required.

You may also use the "session stack" command to access other standalone P330 processors in the stack (those that are not part of a G700 unit).

To "session" over to another G700/P330 in a stack

1. At the **MG-001-1(configure)#** prompt, type `session stack`

The **P330-1(configure)#** prompt appears.

2. At the **P330-1(configure)#** prompt, type `session <mod_num> mgp`

where `<mod_num>` is the next P330 processor in the stack.

If you are currently logged in to the master stack processor, `<mod_num>` would be `2`, for the second G700/P330 processor in the stack.

3. For other G700s in the stack, repeat the steps described previously to install firmware for the stack processor, MGP, and media modules.

Installing G700 firmware in a remote, no stack configuration

If additional G700 media gateways are supported in the configuration, but they are not attached as a stack, then you must configure each G700, with all of its devices, including the P330 processors. Additionally, you must check firmware and update the firmware as required.

Post-upgrade tasks

Stopping IA770 INTUITY AUDIX Messaging, if loading an IA770 update

After the upgrade is complete, perform the following post-upgrade tasks.

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Stop Messaging Software**.

The **Stop Messaging Software** Web page is displayed.

4. Select the **Stop** button.

The shutdown of the messaging server will begin once all users have logged off from IA 770. Once the server has been stopped, the Web page will display status information. Once this process has begun, it will take a few minutes to complete the shutdown.

Installing IA770 service pack (or RFU) files, if any

If IA770 is being used, a post-upgrade service pack for IA770 may be required. See the IA770 documentation for procedures to install a service pack. The service pack file and documentation can be found on the Avaya Support Web Site at <http://support.avaya.com>.

1. Select **Messaging Administration** from the main menu.
2. Select **Utilities** from the Messaging Administration menu.
3. Select **Software Management** from the Utilities menu.
4. Select **Advanced Software Installation** from the Software Management menu.
5. Select **Continue this operation without current system backup**.
6. Select the IA770 update package and click **Install Selected Packages**.

Note:

The system automatically prompts you to restart INTUITY AUDIX when the service pack has been installed. Therefore, if you restart AUDIX at this time, you do *not* need to perform the following procedure, [Starting IA770 INTUITY AUDIX Messaging](#).

Starting IA770 INTUITY AUDIX Messaging

**CAUTION:**

You do *not* need to perform this task if you restarted AUDIX as a part of the installation of the IA770 service pack.

After the IA770 INTUITY AUDIX Messaging application has been updated, you must restart it using the following steps:

1. From the **Maintenance Web Page**, select **Messaging Administration** from the **Miscellaneous** menu.

The **Messaging Administration** Web page is displayed in a new Web browser window.

2. From the **Messaging Administration** Web page, select **Utilities**.

The **Utilities** Web page is displayed.

3. Select **Start Messaging Software**.

The **Start Messaging Software** Web page is displayed. This page will display the status of the system as it starts.

4. When the message, "Startup of the Voice System is complete", is displayed, select the **Return to Main** button and do the next procedure in this document.

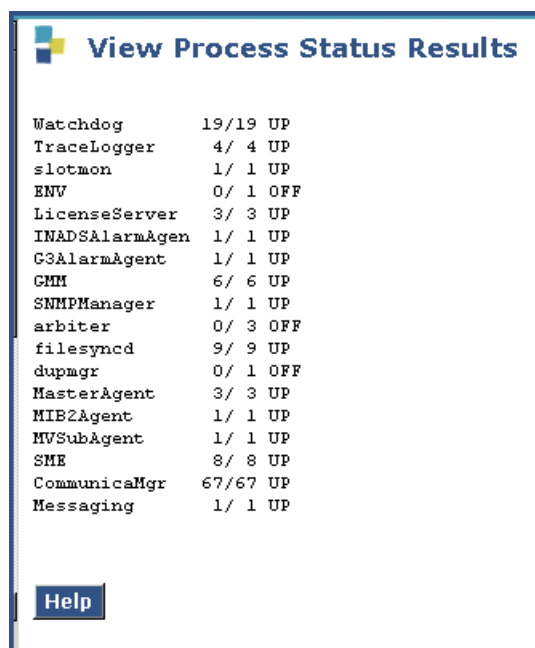
Verifying start up of IA770 INTUITY AUDIX Messaging

To verify operation of IA770 INTUITY AUDIX Messaging, perform the following steps:

1. In the Maintenance Web Interface, under Server, click **Process Status**.
2. Select **Summary and Display once** and click **View**.

the **View Process Status Results** screen displays.

View Process Status screen



Watchdog	19/19	UP
TraceLogger	4/ 4	UP
slotmon	1/ 1	UP
ENV	0/ 1	OFF
LicenseServer	3/ 3	UP
INADSAlarmAgen	1/ 1	UP
G3AlarmAgent	1/ 1	UP
GMM	6/ 6	UP
SNMPManager	1/ 1	UP
arbiter	0/ 3	OFF
filesyncd	9/ 9	UP
dupmgr	0/ 1	OFF
MasterAgent	3/ 3	UP
MIB2Agent	1/ 1	UP
MVSubAgent	1/ 1	UP
SME	8/ 8	UP
CommunicaMgr	67/67	UP
Messaging	1/ 1	UP

[Help](#)

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manager** should show **65/65 UP** or, if IA770 is installed, **67/67 UP**.

The number of processes (67/67) 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 66/67 UP would indicate that a process did not come up and should be investigated before proceeding.

4. Using a telephone, make test calls to verify that call processing is working.
5. Run an IA770 sanity test:
- At the Linux command line, type `/vs/bin/display`
 - All states should be `Inserv` with an associated phone number.
 - Retrieve the test message saved before the upgrade.

Saving translations

To save translations:

- In the SSH session, open a SAT session.
- Log in again as *craft*.

3. Type **save translation** and press **Enter**.

When the save is finished, the system displays the message,
Command successfully completed.

If using IA770, administering switch integration for H.323

The IA770 INTUITY AUDIX Messaging application uses H.323 signaling instead of the CWY1 board for integration with Communication Manager. The tasks for administering the H.323 integration are explained in *Administering Media Servers to work with IA770*.

Testing to verify system functionality

Test the system for functionality, if you are upgrading an S8300 primary controller;

1. Verify the following:
 - Telephones have dial tone
 - You can call from one telephone to another telephone on the system
 - You can make an external trunk call.
 - The media gateways have registered. Use the SAT command **list media-gateway**.

Completing the upgrade process (S8300 is the primary controller)

Telnet to the S8300 (primary controller) and open a SAT session:

1. [To check media modules](#) on page 754
2. [To enable scheduled maintenance](#) on page 754
3. [To busy out trunks](#) on page 754
4. [To check for translation corruption](#) on page 754
5. [To resolve alarms](#) on page 754
6. [To re-enable alarm origination](#) on page 755
7. [Backing up the system](#) on page 755

To check media modules

1. Type `list configuration all` and press **Enter**.
2. Verify that the software is communicating with all media modules and that all media modules are listed in the reports.
3. Make test telephone calls to verify that Communication Manager is working.

To enable scheduled maintenance

1. Type `change system-parameters maintenance` and press **Enter**.
2. Ensure that the **Start Time** and **Stop Time** fields' administration is the same as before the upgrade.

To busy out trunks

1. Busy out trunks that were busied out before the upgrade (see [To record all busyouts](#) on page 702).

To check for translation corruption

1. Type `newterm` and press **Enter**.

If you do not get a login prompt and see the following message:

Warning: Translation corruption detected

follow the normal escalation procedure for translation corruption before continuing the upgrade.

To resolve alarms

1. On the Maintenance Web Interface, under Alarms click **Current Alarms** to examine the alarm log.
2. If any alarms are listed, click **Clear All**.
3. Resolve new alarms since the upgrade through Communication Manager using the appropriate maintenance book.

To re-enable alarm origination

1. Telnet to the S8300 and log on.
2. At the command prompt, type `almenable -d b -s y`,
where
 - d b sets the dialout option to *both* (numbers)
 - s y enables SNMP alarm origination
3. Type `almenable` (without any options) to verify alarm origination enabled status.

Backing up the system

To back up the system to compact flash media (S8300C Media Server only)

1. Plug the cable to the compact flash drive into a USB port on the S8300C.
2. Insert a 128-Mb compact flash media into the top right slot of the drive.
3. On the S8300 main menu, select **Backup Now**.

The system displays the **Backup Now** screen.

4. Select the type of data you want to back up by selecting the appropriate data set.
5. Select Local Compact Flash Card back up the data onto the compact flash card.
Optionally, select Format Compact Flash to format a new card.

Note:

The compact flash card needs to be formatted only before the first use.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

To back up the system over the customer's LAN

1. Make sure you have the IP address of the customer's FTP, SFTP, or SCP backup server.
2. On the S8300 main menu, select **Backup Now**.

The system displays the **Backup Now** screen.

3. Select the type of data you want to back up by selecting the appropriate data set.

4. Select a backup method, normally **FTP**, **SFTP**, or **SCP**, to indicate the destination to which the system sends the backup data.
5. Complete the following fields:

- **User name**

You must enter a valid user name to enable the media server to log in to the FTP or SCP server. If you want to use the anonymous account, type **anonymous** in this field. If you do not want to use the anonymous account, type the actual user name in this field.

- **Password**

You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP or SSH site may have a different convention.

- **Host name**

Enter the DNS name or IP address of the FTP or SCP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

- **Directory**

Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. The default directory for backup data on the FTP or SCP server is /var/home/ftp. If you do not want to use the default directory, you must enter the path name for the directory.

6. Click **Start Backup**.

The system displays the results of your backup procedure on the **Backup Now** results screen.

This completes the installation of the G700 Media Gateway with an S8300 Media Server as primary controller.

Chapter 13: Manual upgrade of an existing G700 without an S8300 to R4.0

This section covers the manual procedures to upgrade the firmware on an existing Avaya G700 Media Gateway without an Avaya S8300 Media Server. The G700 is controlled by an external primary server running Avaya Communication Manager. The primary server can be an Avaya S8500 or S8700-series Media Server or an S8300 residing in another G700.

Note:

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

About the existing G700 upgrade

To upgrade the firmware on an existing Avaya G700 Media Gateway without an Avaya S8300 Media Server, you perform the following major tasks:

1. [Before going to the customer site](#)
2. [On-site preparation for the upgrade](#)
3. [Install new firmware on the G700 Media Gateway](#)

What are the G700 system components

A P330 Stack Processor is built into the G700 Media Gateway. (This processor is also known as the *Layer 2 switching processor*). In addition, the G700 contains:

- Media Gateway Processor (MGP)
- VoIP processor
- Up to four media modules
- Possibly an expansion module

Installing or upgrading the firmware for one or more of these processors and/or media modules is a required part of most new installations or upgrades.

About firmware files

You should obtain the firmware files for the G700 before going on-site. You can obtain the firmware files in bundled form on a CD or you can go to the Avaya Support website and download the individual firmware files onto your services laptop.

About the TFTP server

To install firmware on a G700 without an S8300 or LSP, you must first copy the firmware files to an external TFTP server on the customer LAN. The TFTP server can be a customer computer or it can be set up on your services laptop.

About system access

Accessing the G700

See [About connection and login methods](#) on page 41 for details on how to connect and log into the G700. You can access the G700 in several ways.

Direct connections

- If you are at the location of the primary server, you can connect directly to the Services port on the server and:
 - Open the Web Interface and use the Upgrade Tool.
 - Or, telnet to the server, and then telnet to the P330 stack processor
- If you are at the location of the G700, you can connect directly to the G700 Console port and open a Hyperterm session to access the P330 stack processor.

For direct connections, the TFTP server must be on the customer LAN; *not* on your laptop.

LAN connections

If you can connect to the customer's LAN, you can:

- Use your Internet Explorer browser to access the Web Interface on the primary server and use the Upgrade Tool.
- Telnet to the P330 stack processor and perform the installation commands.

For LAN connections the TFTP server either can be your laptop or a customer computer on the LAN.

Before going to the customer site

Perform the following tasks before going to the customer site:

- [Planning forms that the project manager provides](#) on page 759
- [Setting up the TFTP server on your laptop or on a customer PC, if necessary](#) on page 759
- [Downloading G700 firmware files to your TFTP directory](#) on page 760

Planning forms that the project manager provides

The project manager should provide you with forms that contain all the information needed to prepare for this installation. The information primarily consists of:

- IP addresses
- Subnet mask addresses
- Logins and passwords
- People to contact
- The type of system
- Equipment you need to install

Verify that the information provided by the project manager includes all the information requested in your planning forms.



Tip:

[Appendix B: Information checklists](#), provides several checklists to help you gather the installation and upgrade information.

Setting up the TFTP server on your laptop or on a customer PC, if necessary

A **tar.gz** file, which you obtain from a CD-ROM or a website, contains new G700 firmware. To install the firmware on a G700, you must place this **tar.gz** file on a TFTP server that is connected to the customer's LAN. The TFTP server can be a customer computer, or it can be your laptop, if you have arranged with the customer to connect your laptop to the LAN.

Note:

A Linux or Unix TFTP server should be used only if the customer already has an existing one. In these cases, you download the **tar.gz** file to your laptop and give it to the customer for proper placement and execution.

To obtain the TFTP server software and install it, see [Appendix D: Install the Avaya TFTP server](#).

Downloading G700 firmware files to your TFTP directory

To install new firmware for the G700 processors and the media modules, you first need to move the new firmware files to a directory on the TFTP server. The installation program reads the new firmware files from this directory on the TFTP server.

Perform one of the two procedures in this section, depending on whether you have a bundled tar.gz file on a CD or wish to download individual firmware files from the Avaya Support website.

Downloading individual firmware files

Download the firmware files from the Web to your TFTP directory

Note:

The sequence of links on the website may be somewhat different than described here.

1. Access the <http://www.avaya.com/support> website.
2. Navigate to Firmware Downloads for The G700 Media Gateway.

The system displays a list of firmware files.

3. Locate the file names that match the files listed in your planning documentation.

The file names will approximate those listed in [Table 39](#):

Note:

The latest firmware versions may differ from those listed in [Table 39](#). Also, the appropriate firmware version may depend on the hardware vintage and/or on the release of Communication Manager. See *Communication Manager Software/Firmware Compatibility Matrix* under Downloads on support.avaya.com.

**CAUTION:**

If you are a customer administrator, you might be required to access the **Download Center** Web site in order to download firmware. For instructions on setting up access to the Download Center, access <http://support.avaya.com> and click on the appropriate links.

Table 39: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_1_6.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.6.9.exe
G700 Media Gateway	mgp<version id>	mgp_26_23_1.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v66.fdl
8-port DCP Media Module	mm712<version id>	mm712v8.fdl
24-Port Analog Media Module	mm716<version id>	mm716v86.fdl
24-Port DCP Media Module	mm717<version id>	mm717v6.fdl
8-port/trunk Analog Media Module	mm711<version id>	mm711v17.fdl mm711h7v24.fdl mm711h20v71.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v71.fdl
T1/E1 Media Module	mm710<version id>	mm710v18.fdl
8-port BRI Media Module	mm720<version id>	mm720v7.fdl
2-port BRI Media Module	mm722<version id>	mm722v7.fdl

- Double-click the file name.

The system displays a **File Download** window.

- Click on **Save this file to disk**.
- Save the file to the **C:\tftp** directory (or your alternate tftp location).
- Use WinZip or another zip file tool to unzip the file, if necessary.

On-site preparation for the upgrade

Before installing new firmware on the G700 processors and medial modules you need to prepare on-site by:

- [Accessing the P330 stack processor](#) on page 762
- [Verifying the contents of the tftpboot directory](#) on page 762

as described in this section.

Accessing the P330 stack processor

See [About connection and login methods](#) on page 41 for details on how to set up a connection and login.

Log on to the P330 stack processor using one of the following methods:

- Using a LAN connection, telnet to the IP address of the P330 stack processor and log in.
- If you are *not* using your laptop as the TFTP server, you can connect your Laptop directly to the G700 Console (Serial) Port. Then use HyperTerm or a similar terminal emulation application to log in to the P330 stack processor Command Line Interface (CLI).

You are now logged-in at the Supervisor level with prompt **P330-1(super)#**.

Verifying the contents of the tftpboot directory

Before proceeding with the G700 firmware installation, you should check the */tftpboot* directory on the TFTP server to make sure the firmware versions match those listed in the planning documentation. If they do not, you must copy the correct firmware versions into the */tftpboot* directory using the following procedure:

1. Download the firmware files from the support Website to your laptop.
2. Using the Web Interface on the S8300 Media Server, copy the firmware files from your laptop to the */var/home/ftp/pub* directory on the S8300, or

Alternatively, you can "ftp" the files from your laptop to the *pub* directory.

3. Copy the firmware files from the *pub* directory to the */tftpboot* directory, using the S8300 Media Server command line interface.

To copy firmware files to the /tftpboot directory of an S8300 Media Server, do the following:

- a. Use telnet, Avaya Site Administration, or another tool to access the S8300 Media Server command line.
- b. Log in as craft.
- c. At the Linux prompt, type `cd /var/home/ftp/pub`, and press **Enter**.
- d. The Linux prompt reappears. The current directory has changed to /var/home/ftp/pub.
- e. At the Linux prompt, type `cp <firmware_filename> /tftpboot`, and press **Enter** to copy a single firmware file to the /tftpboot directory. To copy multiple firmware files (most firmware files have an .fdl suffix), use the command `cp *.fdl /tftpboot`.
- f. The Linux prompt reappears. The firmware file or files have been copied to the /tftpboot directory.
- g. Repeat step 4, if necessary, for other firmware files you want to install.
- h. At the Linux prompt, type `cd /tftpboot`.
- i. The Linux prompt reappears. The current directory has changed to /tftpboot.
- j. At the Linux prompt, type `ls`, and press **Enter**.
- k. A list of files in the directory appears.
- l. Check the directory to make sure the firmware files you want to install are listed.

Determining which firmware to install on the G700

Conduct the following procedure to compare software versions running on the G700 processors and media modules with the versions in you planning documents. If the versions do not match, you need to install the new firmware for those components.

To determine if new firmware for the P330 stack processor is necessary

1. At either the **P330-1(super)#** or **P330-1(configure)#** prompt, type `dir`.

The system displays the directory list of software for the P330 stack processor.

Directory list for P300 stack processor

M#	file	ver num	file type	file location	file description
--	----	-----	-----	-----	-----
1	module-config Configuration	N/A	Running Conf	Ram	Module
1	stack-config	N/A	Running Conf	Ram	Stack Configuration
1	EW_Archive	4.0.4	SW Web Image	NV-Ram	WEB Download
1	Booter_Image	3.2.5	SW BootImage	NV-Ram	Booter Image

Manual upgrade of an existing G700 without an S8300 to R4.0

2. Check the version number (ver num) of the EW_Archive file to see if it matches the Release Letter.

If not, you must upgrade the P330 stack processor.

3. Type **show image version**

The system displays the list of software.

Show image version List for P330 stack processor

Mod	Module-Type	Bank	Version
-----	-----	----	-----
3	Avaya G700 media gateway	A	0.0.0
3	Avaya G700 media gateway	B	4.0.17

4. Check the version number of the stack software image file in Band B to see if it matches the your planning document.

If not, you must upgrade the P330 stack processor.

To determine if new firmware is required for the MGP, VoIP module, and installed media modules

1. Type **session mgp**
2. At the **MG-001-1(super)#** prompt, type **show mg list_config**

The system displays the list of software.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (B)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

3. Refer to the list to check the FW vintage number of the G700.

In the TYPE column, find G700, then check the matching field in the FW VINTAGE column to see if it matches the vintage number in your planning forms. If not, you must install new firmware on the G700 media gateway. Also check if the release number in the FW VINTAGE column contains (A) or (B) to designate the software bank. If the list shows B, you will upgrade A. If the list shows A, you will upgrade B.

4. Refer to the VOIP FW column and row for slot V0 (same row occupied by the G700 information) to see if the number matches the VoIP firmware identified in your planning forms.

If not, you must also upgrade the G700 media gateway motherboard VoIP module.

Note:

The VoIP processor on the motherboard is upgraded using the same firmware image file as the VoIP media modules; for example, the file mm760v8.fdl is vintage #8.

5. Check the FW VINTAGE column for vintages of each of the installed media modules: MM710, MM711, MM712, MM720, and/or MM760 to see if they match the FW vintages in the planning forms.

If not, you must upgrade them, as well.

Install new firmware on the G700 Media Gateway



Important:

The procedures in this section copy firmware files from a TFTP server to the G700. The TFTP server can be an S8300 primary controller, a customer server, or the technician's laptop (if TFTP server software is installed). Before starting this procedure, ensure that:

- The firmware files have been stored on the TFTP server.
- The G700 has connectivity to the TFTP server over the customer's LAN.

If the TFTP server is on the laptop, and the laptop is not connected to the LAN, you can administer a private network between the laptop and G700 with a physical connection through one of the Ethernet ports on the G700.

Manually installing G700 and media modules firmware

Follow the procedures in this section to install firmware on the G700 processors and media modules manually:

- [Installing new firmware on the P330 stack processor](#) on page 766
- [Installing new firmware on the G700 Media Gateway Processor](#) on page 766
- [Installing new firmware on the media modules](#) on page 768

Installing new firmware on the P330 stack processor

To install P330 stack processor firmware

1. At the **P330-1(configure)#** prompt, type

```
copy tftp SW_image <file> EW_archive <ew_file>
<tftp_server_address> <Module#>
```

where *<file>* is the full-path name for the image file with format and vintage number similar to viisa3_8_2.exe,

<ew_file> is the full-path name for the embedded web application file with format similar to p330Tweb.3.8.6.exe,

<tftp_server_ip_address> is the IP address of the TFTP server, and

<Module#> is the number, 1 through 10, of the media gateway in the stack. If there is only one G700 media gateway, the number is 1.

2. Verify that the download was successful when the prompt returns:
 - a. type **show image version <module #>** and check the version number in the Version column for Bank B.
 - b. type **dir <module #>** and check the version number in the ver num column for the EW_Archive file.
3. Type **reset <module #>**.

Installing new firmware on the G700 Media Gateway Processor

To install MGP firmware

1. At the **P330-1(configure)#** prompt, type **session mgp** to reach the G700 media gateway processor.
2. Type **configure** at the **MG-???-1(super)#** prompt to enter configuration mode, which will change the prompt to **MG-???-1(configure)#**.
3. At the **MG-???-1(configure)#** prompt, type **show mgp bootimage** to determine which disk partition (bank) is in the **Active Now** column.

You will update the bank that is *not* listed as Active Now. The system displays the following screen:

Example: Show mgp bootimage

<u>FLASH MEMORY</u>	<u>IMAGE VERSION</u>
Bank A	109
Bank B	210
 <u>ACTIVE NOW</u>	 <u>ACTIVE AFTER REBOOT</u>
Bank B	Bank B

4. At the **MG-???-1(configure)#** prompt, type

```
copy tftp mgp-image <bank> <filename> <tftp_server_ip_address>
```

to transfer the mgp image from the tftp server to the G700,

where

<bank> is the bank that is *not* Active Now (Bank A in the example).

<filename> is the full path name of the mgp firmware image file, which begins with mgp and will be similar to the name mgp_8_0.bin.

<tftp_server_ip_address> is the IP address of the S8300.

For example:

```
copy tftp mgp-image a mgp_8_0.bin 195.123.49.54
```

The screen shows the progress.

5. Type **set mgp bootimage <bank>**

where <bank> is the same letter you entered in the previous step.

6. At the **MG-???-1(configure)#** prompt, type **reset mgp**.

A system prompt asks you to confirm the reset.

7. Select **Yes** at the dialog box that asks if you want to continue.

The G700 media gateway processor resets. The LEDs on the G700 media gateway and the media modules flash. These elements each conduct a series of self-tests. When the LEDs on the media modules are extinguished and the active status LEDs on the G700 media gateway are on, the reset is complete.

8. When the **P330-1(super)#** prompt appears, type **session mgp**.

9. At the **MGP-???-1(super)#** prompt, type **configure**.

10. Verify that the download was successful when the prompt returns.

Type **show mg list_config**.

The system displays the list of software.

Example: Show mg list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	230 (A)	67
V1	ICC	S8300	A	72	00	N/A
V2	DCP	MM712	A	2	58	N/A
V3	ANA	MM711	A	2	57	N/A
V4	DS1	MM710	A	1	58	N/A

Installing new firmware on the media modules

For upgrades of active media modules, you need to take the media modules out of service before initiating the upgrade process. To do this, go to a SAT session on the primary controller and issue a **busyout** command.

Note:

Skip this busyout procedure if the media modules are not in service; for example during an initial installation.

To busyout board (for active media modules)

1. Go to a SAT session on the primary controller and enter the command,
busyout board vx
where **x** is the slot number of the media module to be upgraded.
2. Verify the response,
Command Successfully Completed
3. Repeat for each media module to be upgraded.

To install media module firmware

1. Be sure that you have checked for the current vintage of the VoIP Module for the v0 slot (on the G700 motherboard).
This VoIP module does not occupy a physical position like other media modules.
2. At the **P330-1(configure)#** prompt, type **session mgp**.
3. At the **MG-001-1(super)#** prompt, type **configure** to change to the configuration mode.

4. Type `copy tftp mm-image v<slot #> <filename mm>
<tftp_server_ip_address>`

where

`<slot #>` is the slot of the specific media module,

`<filename mm>` the full-path name of the media module firmware file in a format such as mm712v58.fdl, and

`<tftp_server_ip_address>` is the ip address of the S8300.

Two or three minutes will be required for most upgrades. The VoIP media module upgrade takes approximately 5 minutes. Screen messages indicate when the transfer is complete.

5. After you have upgraded all the media modules, verify that the new versions are present.

At the **MG-???-1(configure)#** prompt, type `show mg list_config`

The list of software appears.

Show MG list_config

SLOT	TYPE	CODE	SUFFIX	HW VINTAGE	FW VINTAGE	VOIP FW
----	-----	-----	-----	-----	-----	-----
V0	G700	DAF1	A	00	21.25.0 (A)	26
V1	ICC	S8300	A	00	5	N/A
V2	DCP	MM712	A	2	5	N/A
V3	ANA	MM711	A	3	16	N/A
V4	DS1	MM710	A	1	8	N/A

6. In the **TYPE** column, find the particular media module (v1 through v4), then check the matching field in the **FW VINTAGE** column to see if it matches the planning documentation.

Note:

Slot V1 can contain either a media module or the S8300, which will show as
TYPE ICC.

7. Check the **VOIP FW** column and row for slot v0 to see if the number matches the VoIP firmware identified in the planning documentation.
8. Type `reset <module #>`
where `<module #>` is the number of the G700 in the stack.
9. When the reset is finished, type `show mm` to verify the upgrade.

To release board (if media module was busied out)

1. When the upgrade procedure is complete, go to the SAT session and release the board

Type **release board vx**

where **x** is the slot number of the upgraded media module.

2. Verify the response,

Command Successfully Completed

Note:

If you see the response, Board Not Inserted, this means that the media module is still rebooting. Wait one minute and repeat the **release board** command.

3. Repeat the **release board** command for each media module that was busied out.

Ensuring the MGP default gateway IP address is set

Communication Manager release 4.0 requires that the built-in VoIP module of the G700 Media Gateway has a default gateway IP address. To ensure that this IP address is set, perform the following steps:

1. At the **MG-???-1(configure)#** prompt, type **show ip route mgp**.

The list of mgp routes appears.

MG-001-1(super)# show ip route mgp				
DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	135.9.80.254	motfec0	(3/0/165)
135.9.80.0	255.255.255.0	135.9.80.88	motfec0	(101/0/0)
MG-001-1(super)#				

2. Check that a Gateway IP address exists for Destination 0.0.0.0.
3. If a Gateway IP address does not exist, type, at the **MG-???-1(configure)#** prompt, **set ip route 0.0.0.0 0.0.0.0 <IP_address>**, where **<IP_address>** is the default gateway IP address.

After you reboot the media gateway, the IP address is active and available.

Setting rapid spanning tree on the network

Spanning Tree (STP) is a loop avoidance protocol. If you don't have loops in your network, you don't need STP. The "safe" option is always to leave STP enabled. Failure to do so on a network with a loop (or a network where someone inadvertently plugs the wrong cable into the wrong ports) will lead to a complete cessation of all traffic. Rapid Spanning Tree is a fast-converging protocol, faster than the earlier STP, that *enables* new ports much faster (sub-second) than the older protocol. Rapid Spanning Tree works with all Avaya equipment, and can be *recommended*.

Rapid Spanning Tree is set using the P330 stack processor command line interface.

To enable/disable spanning tree

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press **Enter** to display the set spantree commands selection.
3. To enable Spanning Tree, type **set spantree enable** and press **Enter**.
4. To set the **rapid spanning tree** version, type **set spantree version rapid-spanning-tree** and press **Enter**.

The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). In order to avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **set port spantree cost auto**.

Note:

Avaya P330s now support a "Faststart" or "Portfast" function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop.

To set an **edge-port**, type **set port edge admin state module/port edgeport**.

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User's Guide* (available at <http://www.avaya.com/support>).

This completes the G700 firmware upgrade procedures.

Appendix A: Technical information

This appendix collects some of the detailed technical information you will need to install the Avaya G700 Media Gateway with an Avaya S8300 Media Serve. More complete information can be found in *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207.

Avaya G700 Media Gateway Technical Specifications

[Table 40: Technical Specifications](#) provides detailed information on the physical dimensions and tolerances of the G700 Media Gateway.

Table 40: Technical Specifications

Chassis Dimensions

Height	2U (3.5 in)	88 mm	Depth	17.7 in	450 mm
Width	19 in	482.6 mm	Weight empty	22.25 lbs	10 kg
			Weight	34-27 lbs	16-12 kg

Required Clearances

Front	12 in	30 cm	consistent with EIA 464 data rack standards
Rear	18 in	45 cm	

Temperature Tolerances

Recommended	65 to 85 deg Farenheit		18 to 29 deg Celsius	
Continuous operation	+41 deg F to +104 deg F		5 deg C to 40 deg C	
BTU per Hr	1218			

1 of 2

Table 40: Technical Specifications (continued)

Voltage and Current

AC	100–240 VAC, 50–60 Hz, 5A Max
DC	-48 VDC, 8A Max
Circuit Breaker	15 amp

Humidity Tolerances

Recommended	20 to 60% relative humidity
Relative humidity range	10% to 90% non-condensing

Altitude

Recommended	up to 10,000 feet or 3,000 meters

2 of 2

Cabling Equipment

[Table 41: Media Gateway Cables and Peripherals](#) lists the types and specifications of the cables used to connect the Media Gateway. See also *Avaya P333T User's Guide*.

Table 41: Media Gateway Cables and Peripherals

Cable	Description	Length	Length (metric)
X330SC Short Octaplane™ Cable (30 cm) (Catalog No. CB0223)	Short Octaplane cable - light-colored, used to connect adjacent switches or switches separated by one Backup Universal Power Supply (BUPS) unit.	12 in	30 cm
X330LC Long Octaplane Cable (2 m) (Catalog No. CB0225)	Long Octaplane cable - light-colored, used to connect switches from two different physical stacks	6 ft	2 m

1 of 2

Table 41: Media Gateway Cables and Peripherals (continued)

Cable	Description	Length	Length (metric)
X330RC Redundant Octaplane Cable (2 m) (Catalog No. CB0222)	Redundant cable - black, used to connect the top and bottom switches of a stack.	6ft	2 m
X330L-LC Extra Long Octaplane Cable (8 m) (Catalog No. CB0270)	Extra-Long Octaplane cable - light-colored, used to connect switches from two different physical stacks	24 ft	8 m
X330L-RC Long Redundant Octaplane Cable (8 m) (Catalog No. CB0269)	Long Redundant cable - black, used to connect the top and bottom switches of a stack.	24 ft	8 m
Stacking Sub-Module X330STK	Stacking Sub-Module provides two backplane links		

2 of 2

Appendix B: Information checklists

This appendix is can be used as an aid for collecting necessary information for the installation of a G700 Media Gateway and an S8300 Media Server.

The following lists are provided:

- [Installer's Checklist](#):: Tools, software, laptop settings, customer network information.
- [Serial Number and Login Information](#): Serial numbers of the G700s and login/passwords for various access methods.
- [Set-Up for P330 Stack Processor](#): IP addresses and setup commands for the P330 stack processor.
- [Set Up for G700 Media Gateway Processor \(MGP\)](#): IP addresses and setup commands for the MGP.
- [Set Up for VoiP Resources](#): IP addresses, slot numbers, and setup commands for the VoIP media modules.
- [Set Up for S8300 Media Server](#): IP addresses and setup commands for the S8300.
- [Installation Site Information](#): Customer and site contact information
- [Stack Layout](#): G700 stack arrangement and slot assignments.

Installer's Checklist

	tools
	laptop with 32 MB RAM
	40 MB available disk space
	RS-232 port connector
	cross-over Ethernet cables
	direct Ethernet cable
	serial cable and adapter
	Ethernet network connection (NIC card)
	screwdriver
	software
	Windows 95/98/ME/XP/NT/2000 operating system
	FTP Program
	TFTP Program
	Telnet Program
	Terminal emulation program: HyperTerminal or other
	TCP/IP networking software: bundled with Windows OS
	Web browser: Netscape 4.7x or Internet Explorer 5.0
	Ethernet connections
	laptop default address and mask: 192.11.13.5, 255.255.255.252
	Browser: no proxies
	laptop default address and mask: 192.11.13.5, 255.255.255.252
	Communications Properties: 9600 baud rate; no parity; 8 data bits, 1 stop bit; no
	SSO login
	Obtaining this login will require that you complete the authentication process. You will not be able to obtain the license file or to perform remote feature activation without the SSO login authentication process. You will not be able to obtain the license file or to perform remote feature activation without the SSO login.
	dial plan
	IP addressing plan
	List of customer-provided IP services

Serial Number and Login Information

G700 Serial Numbers

Logins

	Name & Password
S8300 Media Server	
P330 Stack	
G700 Media Gateway	
SSO Authentication Login	
ftp	anonymous
	email address
Communication Manager	

Set-Up for P330 Stack Processor

Located in G700 Media Gateway#

Prompt: **P330-1(super)#** type `configure` to change prompt to: **P330-1(configure)#**
 For the Stack Master:

Command	Requested Field	Information to be Entered
<code>set interface inband</code>	<i>vlan</i>	1
	<i>IP address</i>	
	<i>netmask</i>	
<code>set ip route</code>	<i>destination IP address</i>	
	<i>gateway IP address</i>	
<code>set time protocol</code>	<i>sntp-protocol / time-protocol</i>	
<code>set time server</code>	<i>IP address of time server</i>	
<code>set timezone</code>	<i>zone name</i>	
	- <i><hours></i> (offset from GMT)	

Set Up for G700 Media Gateway Processor (MGP)

G700 Media Gateway

Prompt:

MG-???-n (super)# type `configure` to change prompt to **MG-???-n (configure)#**

Command	Requested Field	Information to be Entered
set interface mgp	<i>vlan</i>	1
	<i>IP address</i>	
	<i>netmask</i>	
	<i>gateway IP address</i>	
set hostname	<i>hostname</i>	
set ip route	<i>destination IP address</i>	
	<i>gateway IP address</i>	
set mgc list	<i>IP address</i>	
	<i>IP address</i>	
	<i>IP address</i>	
	<i>IP address</i>	
show system	<i>serial number</i>	

Set Up for VoIP Resources

G700 Media Gateway #

Command	Requested Field	Information to be Entered
<code>set interface voip</code>	<i>number</i>	V0 for resident VoIP resource of the G700
	<i>ip address</i>	
	number (v + slot #)	
	ip address	
	number (v + slot #)	
	ip address	
	number (v + slot #)	
	ip address	
	number (v + slot #)	
	ip address	

G700 Media Gateway #

Command	Requested Field	Information to be Entered
<code>set interface voip</code>	<i>number</i>	V0 for resident VoIP resource of the G700
	<i>ip address</i>	
	number (v + slot #)	
	ip address	
	number (v + slot #)	
	ip address	
	number (v + slot #)	
	ip address	
	number (v + slot #)	
	ip address	

Set Up for S8300 Media Server

Location: slot #1 of G700

survivable processor?

Web Interface: 192.11.13.6 (default)

Screen Title	Field	Information to be Entered
Login	Name	
	Password	
Set Time and Date	Time & Date	
Configure Server Set Server Identities	hostname	
	Server IP address	
	Server netmask	
	default gateway IP address	
	Ethernet interface IP address (IA770)	
	Ethernet interface netmask (IA770; same as Server netmask)	
Configure VLAN	VLAN ID	
	IP address	
	gateway IP address	
	netmask	
DNS Server Configuration	Enable/Disable DHCP	Disable
Network Time Server	Enable/Disable NTP	
	IP addresses of designated Network Time Servers	
	Trusted Key, Requested Key, Control Key	leave blank
	Do Not Install a New Keys File	Default
Set Modem Interface	IP address	

Installation Site Information

Site Name	Main Phone
Installation Address	
Shipping Address	
Customer Contact	Name Title Phone: FAX: Mobile: Pager: email: Off-hours contact:
Salesperson/ Account Exec	Sales/AE phone: Other Contact Info:
Notes to installer: access procedures, safety/security procedures	
Access Contact	Name Title Phone: FAX: Mobile: Pager: email: Off-hours contact:
Installer Name Date of Installation	

Stack Layout

Label each unit in the stack. Make photocopies if needed. There can be no more than 10 units per stack.

Media Gateway (module) #
or C360 switch #

v1	v2
	v3
Expansion Module	v4

Media Gateway (module) #
or C360 switch #

v1	v2
	v3
Expansion Module	v4

Media Gateway (module) #
or C360 switch #

v1	v2
	v3
Expansion Module	v4

Media Gateway (module) #
or C360 switch #

v1	v2
	v3
Expansion Module	v4

Appendix C: Equipment list

The following lists contain information necessary for ordering Avaya G700 Media Gateway and Avaya S8300 Media Server equipment.

Note:

If ordering parts, use the 9-digit "Comcode" numbers, not the 6-digit numbers.

Table 42: Equipment List: Avaya S8300 Media Server with G700 Media Gateways

Avaya G700 Media Gateway

The Avaya G700 Media Gateway is a 19-inch 2u rack-mountable device with a physical design modeled after the Avaya P330 stackable switching products. The G700 Media Gateway contains VoIP resources, a layer 2 switch, modular interface connectivity for traditional trunk and station access and performs the function of a gateway/gatekeeper. It also houses four Media Module Bays as well as a single, standard Avaya Expansion Module interface slot. The Avaya G700 Media Gateway is designed to offer options and scalability. A customer will be able to mix and match Media Modules, as well as stack and/or add additional Avaya G700 Media Gateways as they grow in size.

Material Code: 170896	Apparatus Code: MGW1	Not Optional

Avaya G700 Media Gateway Comcode (for Services Ordering Only)

Comcode	Number of Items	Description
700394984	1	G700 Media Gateway (AC/DC version)
700017932	1	Rack mount screw set (attach ears to rack)
700316425	2	Rack Mount Ears
901342105	6	Rack Mount screw set ear to box
700051055	4	Feet
700169998	1	Tech Laptop Cable
700316409	3	Media Module Blanks
700316367	1	Avaya Expansion Blank
700179203	1	Avaya Octaplane Blank

1 of 2

Table 42: Equipment List: Avaya S8300 Media Server with G700 Media Gateways (continued)**Avaya G700 Media Gateway**

700179526	1	Documentation, CIB 3246 FCC/ Safety G700
700236680	0	Grounding Kit for multiple G700s in a 19" rack
2 of 2		

Table 43: Equipment List: G700 Media Gateway Power Cords**G700 Media Gateway Power Cords**

Supplies Power to the G700 Media Gateway. One cord per gateway is required, and there are various cords depending on the power required for the country in which the unit will be installed.

Material Code: 170904	Apparatus Code: none	Not Optional

When you order this material code, a descriptive attribute will be required; the attributes are:

Attribute	Option	Comcode: Description
CRD	30	405362641: PWR CORD 9X10 IN USA 17505
CRD	31	407786623: PWR CORD 98IN EUROPE 12013S
CRD	32	407786599: PWR CORD 98IN UNITED KINGDOM 14012
CRD	33	407786631: PWR CORD 98IN AUSTRALIA 15012
CRD	34	407790591: PWR CORD INDIA P250CIM
CRD	42	408161453: PWR CORD 96IN ARGENTINA
CRD		700252638: DC PWR CORD

Table 44: Equipment List: Avaya S8300 Media Server

Server
S8300B Media Server
The Avaya S8300 Media Server is an Intel™-based server complex that carries: ● Avaya Communication Manager ● administration and maintenance provisioning software ● Hard drive (Field-replaceable. Comcode: 700307028) ● 512 MB RAM ● Web serve ● Linux OS ● H.248 Media Gateway Signaling Protocol ● CCMS messages tunneled over H.248 Signaling Protocol ● TFTP server The S8300 Media Server can act as the primary server of the G700 Media Gateway, or it can serve as a local survivable processor for remote/branch customer locations.
Comcode (for Services Ordering Only): 700335144

Table 45: Equipment List: Avaya S8300 Media Server

Server
S8300C Media Server
The Avaya S8300 Media Server is an Intel™-based server complex that carries: ● Avaya Communication Manager ● administration and maintenance provisioning software ● Hard drive (Field-replaceable. Comcode: 700307028) ● One GB RAM ● Web serve ● Linux OS ● H.248 Media Gateway Signaling Protocol ● CCMS messages tunneled over H.248 Signaling Protocol ● TFTP server The S8300 Media Server can act as the primary server of the G700 Media Gateway, or it can serve as a local survivable processor for remote/branch customer locations.
Comcode (for Services Ordering Only): 700407810

Table 46: Equipment List: Media Modules

Media Modules		
MM710 T1/E1 Media Module		Comcode (for Services Ordering Only): 700394737
The MM710 T1/E1 Media Module offers the combined features of a DEFINITY DS1 circuit pack and will include the following: ● A built-in CSU ● AMI-BASIC ● Both A-law for E1 and μ -law for T1 ● Line Coding: AMI, ZCS, B8ZS for T1 and HDB3 or AMI for E1 ● Stratum 3 Clock compatibility ● Trunk signaling for supporting US and International CO trunks and tie trunks as currently in existence The MM710 T1/E1 Media Module supports the universal DS1 conforming to 1.544 Mbps T1 standard and 2.048 Mbps E1 standard ISDN PRI is also supported for T1 or E1 revenue-associated option. The MM710 is RoHS compliant.		
DEF DS1 LOOPBACK JACK 700A		
Provides the ability to remotely troubleshoot the MM 710 T1/E1 Media Module. It is required for any customer with a maintenance contract and highly recommended for any other customer.		
Material Code: 107988867	Apparatus Code: None	Required for any customer with a maintenance contract and an MM710 T1/E1 Media Module, highly recommend for other customers to avoid expensive technician visits.

1 of 4

Table 46: Equipment List: Media Modules (continued)

Media Modules	
MM711 Analog Media Module	Comcode (for Services Ordering Only): 700394661
The MM711 Analog Media Module supports eight analog interfaces allowing the connectivity of Loop Start, Ground Start, Analog DID trunks, and 2-wire analog Outgoing CAMA E911 trunks. As well, the MM711 Analog Media Module allows connectivity of analog, tip/ring devices such as single line telephones, modems or group 3 fax machines. Each port may be configured as either a trunk interface or a station interface. Also included is support for caller ID signaling, ring voltage generation for a variety of international frequencies and cadences and administrable line termination styles. The MM711 is RoHS compliant.	
MM714 Analog Media Module	Comcode (for Services Ordering Only): 700395221
The MM714 Analog Media Module supports four analog stations and four CO trunks. Analog DID trunk connections are to be associated with the ports labeled "Line" and not "Trunk". The MM714 is RoHS compliant.	
MM712 DCP Media Module	Comcode (for Services Ordering Only): 700394745
The MM712 DCP Media Module allows connectivity of up to 8 two-wire DCP voice terminals. MM712 will not support 4-Wire DCP telephones. Signal timing specifications for the MM712 support TDM Bus Timing in receive and transmit modes. The G700 Media Gateway supplies only +5 VDC and –48 VDC to the MM712 Media Module. Any other required voltages must be derived on the module. Loop range secondary protection is provided on the MM712. The MM712 is also self-protecting from an over current condition on a tip and ring interface. The MM712 is RoHS compliant.	
MM716 24 port Analog Media Module	Comcode (for Services Ordering Only): 700394703
The MM716 provides 24 analog ports supporting telephones, modem, and fax. These ports can also be configured as DID trunks with either wink-start or immediate-start. The 24 ports are provided via a 25 pair RJ21X amphenol connector, which can be connected by an amphenol cable to a breakout box or punch down block. The MM716 is RoHS compliant.	
2 of 4	

Table 46: Equipment List: Media Modules (continued)

Media Modules

MM717 24 port DCP Media Module	Comcode (for Services Ordering Only): 700394711

The MM717 DCP Media Module supports 24 DCP stations. The MM717 uses a 25-pair amphenol connector on the media module's faceplate. The 24 DCP ports are intended for in-building use only. Phone lines connected to those ports are not to be routed out-of-building. Failure to comply with this restriction could cause harm to personnel or equipment. The MM717 is RoHS compliant.

NOTE: No more than 3 MM717 Media Modules can be installed in a single G700.

MM720 BRI Media Module	Comcode (for Services Ordering Only): 700394752

The MM720 BRI Media Module contains eight ports that can be administered either as BRI trunk connections or BRI endpoint (telephone and data module) connections. Information is communicated in two ways:

Over two 64 Kbps channels called B1 and B2 that can be circuit-switched simultaneously

Over a 16 Kbps channel called the D channel that is used for signaling. The D channel occupies one time slot for all eight D channels.

The circuit switched connections have a u-law or A-law option for voice operation. The circuit switched connections operate as 64 Kbps clear channels when in the data mode.

The MM720 BRI Media Module does not support combining both B channels together to form a 128 Kbps channel.

Note:

The MM720 BRI Media Module cannot be administered to support both BRI trunks and BRI endpoints at the same time.

For BRI trunking, the MM720 BRI Media Module supports up to eight BRI interfaces, or up to 16 trunk ports, to the central office at the ISDN S/T reference point.

For BRI endpoints, each of the 8 ports on the MM720 BRI Media Module can support one integrated voice/data endpoint or up to 2 BRI stations and/or data modules. Supported endpoints must conform to AT&T BRI, World Class BRI, or National ISDN NI1/NI2 BRI standards. The MM720 BRI Media Module provides -40 volt phantom power to the BRI endpoints.

The MM720 is RoHS compliant.

Table 46: Equipment List: Media Modules (continued)

Media Modules	
MM722 2-port BRI Media Module	Comcode (for Services Ordering Only): 700395239
The MM722 BRI Media Module supports two BRI ports. The MM722 is RoHS compliant.	
MM760 VoIP Media Module	Comcode (for Services Ordering Only): 700394760
The MM760 VoIP Media Module is a clone of the motherboard VoIP engine. It provides an additional 64 VoIP channels with G.711 compression. Each chassis base system can support up to 64 G.711 single channel calls. If the desire is to have an essentially non-blocking system, an additional MM760 VoIP Media Module needs to be added if more than two MM710 T1/E1 Media Modules are used in a single chassis. This will provide for an additional 64 channels. This VoIP conversion resource in the G700 Media Gateway is an improved version of the Prowler board resource and from a configuration perspective, the two are the same. The capacity is 64 G.711 TDM/IP simultaneous calls, or 32 compression codec (G.729, G.726, or G.723) TDM/IP simultaneous calls. These call types can be mixed on the same resource, so we say that the simultaneous call capacity of the resource is 64 "G.711 Equivalent Calls". The MM760 is RoHS compliant.	
4 of 4	

Table 47: Avaya P330 Equipment**Avaya P330 Equipment**

Avaya P330 Stacking Sub-Module (optional)		
Material Code: 700397482	P330 MOD P330 STACKING. The P330 Stacking Sub-Modules is RoHS-compliant.	
CASCADE CABLES		
Material code: 700397474	Avaya P330 CABLE OCTAPLANE STACKING 1FT. The P330 one-foot cable is RoHS-compliant.	
Material code: 700397433	Avaya P330 CABLE OCTAPLANE STACKING 6FT. The P330 six-foot cable is RoHS-compliant.	
Material code: 700397466	Avaya CABLE ASSY X330RC REDUN STACKING. The X330RC is RoHS-compliant.	
EXPANSION MODULES		
Material code: 700397490	Avaya MOD P330 10/100TX UPLINK 16PT	The X330-T16 adds 16 10/100Base-T ports. It allows up to 64 ports in a single switch and an impressive 640 per stack. Two LAGs can be created, with up to eight ports per group. The X330-T16 is RoHS-compliant.
Material code: 700397417	Avaya P330 MOD EXP GBIC 2PT	The X330-G2 provides GBIC connectivity with an adapter for standard GBIC transceivers. The X330-G2 is RoHS-compliant.
Material code: 700397409	Avaya X330 WAN-2DS1	The X330 WAN-2DS1 provides two T1/E1 ports and a 10/100BaseT port. The X330 WAN-2DS1 is RoHS-compliant.
1 of 2		

Table 47: Avaya P330 Equipment (continued)**Avaya P330 Equipment**

Material code: 700247570	Avaya X330 WAN-2USP	The X330 WAN-2USP provides two serial ports supporting V.35, X.21, RS530 and a 10/100BaseT port. The X330 WAN-2DS1 is RoHS-compliant.
Material code: 700397383	V.35 DTE Cable	Used with the X330 WAN-2USP.

2 of 2

Appendix D: Install the Avaya TFTP server

This appendix describes the procedure to install and configure the Avaya TFTP server on a technician's laptop or other computer. You can use the capabilities of the TFTP server as the "source" to install software on the S8300 and install firmware on the G700 or G350 Media Gateways and the gateway media modules.

To install the Avaya TFTP server

Create a tftpboot directory

1. Skip this step if you intend to use your CD-ROM drive as the source location for the system software files. Otherwise, on the hard drive of your laptop or the customer's PC, create a directory into which you will load the system software. It is recommended that you create a directory called C:\tftpboot.

Download the TFTP software

The TFTP server software may be available on the Communication Manager software distribution CD in \pc-software\TFTP. If so, skip to Step 8.

2. Connect to the LAN using a browser on your laptop or the customer's PC and access the Avaya Support website on the Internet:
<http://www.avaya.com/support>

3. At the Avaya support site, select the following sequence of menu options:

> Software & Firmware Downloads

scroll down to the **Telephones and End User Devices** category and select

> 4600 Series IP Telephones

> Software Downloads

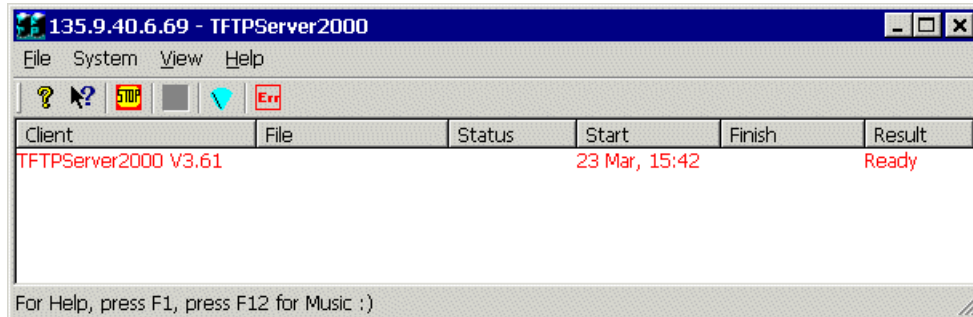
4. >Double-click on one of the links listed with "TFTP Server"; for example, **4630/4630SW IP Telephone R 2.0.1 and TFTP Server**.
5. Scroll to bottom of page to find the TFTP Server Application file, **iptel_avaya_tftp.exe**.
6. Double-click on the filename and download the file to your laptop or the customer PC that will serve as the TFTP server. The directory that you download this file to can be a temporary directory — it is not the directory that the TFTP server will be installed in. Remember this directory.
7. You may also wish to download and view or print the file **iptel.pdf**, which provides instructions on installing the **iptel_avaya_tftp.exe** for Windows servers.

Install the Avaya TFTP server

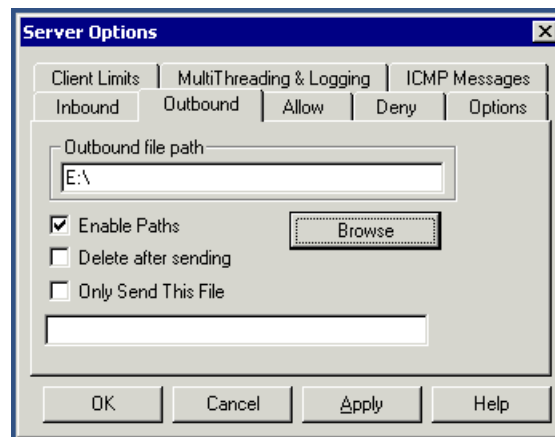
Install the TFTP software

8. After downloading the **iptel_avaya_tftp.exe** file, double-click it and follow the installation instructions. The installation program creates the default installation directory C:\Program Files\Walusoft\TFTPSuite.
9. When the file has been installed, go to the directory where the software was installed and double-click the file **tftpserver32.exe** to open the program.

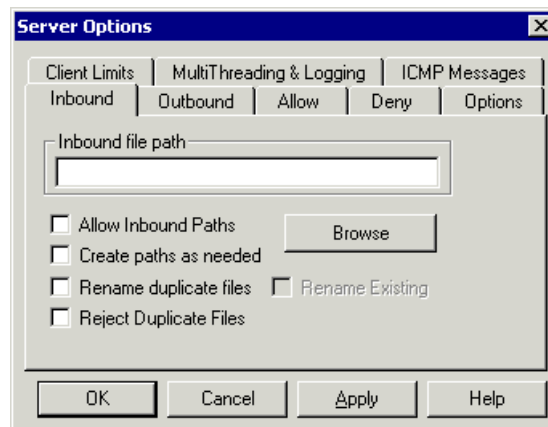
The TFTP Server window appears. The IP address of the PC plus port 69 shows in the top border.



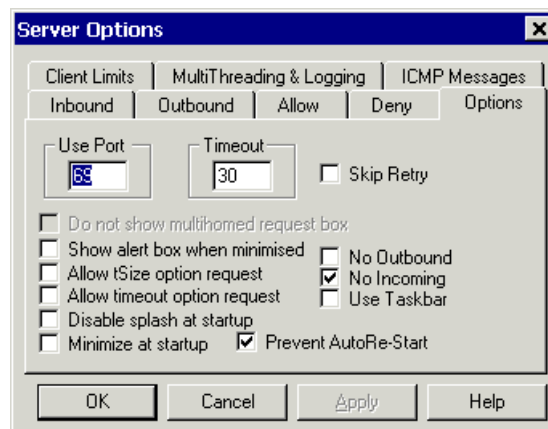
10. Configure the TFTP server as follows:
 - a. Click on **System** from the menu bar and select **setup**.
 - b. In the **Server Options** window, select the **Outbound** tab, and browse to your CD-ROM drive location and double-click to enter in the outbound file path.



- c. Select the **Inbound** tab and ensure that the Inbound file path is blank



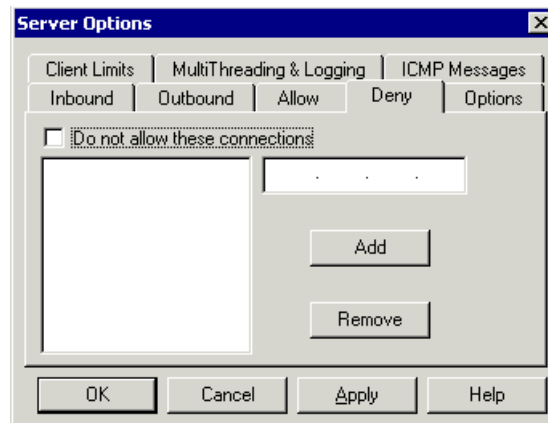
- d. Select the **Options** tab. Enter **69** in the **Use Port** field and **30** in the **Timeout** field.
- e. Select **No Incoming**. However, if you wish to copy files as a backup prior to performing an upgrade of software, leave this field unchecked.
- f. Select **Prevent AutoRe-Start**.



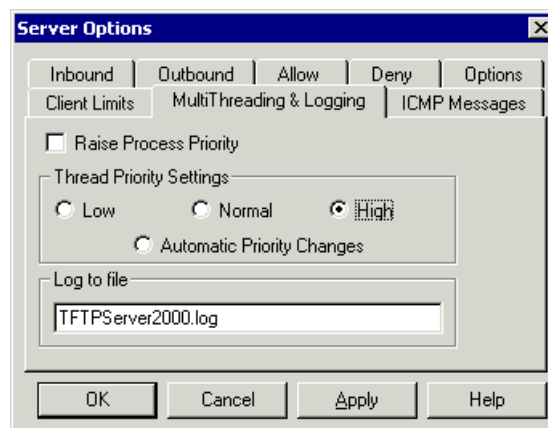
- g. In the **Allow** tab, leave the **Only allow these connections** checkbox unchecked.

Install the Avaya TFTP server

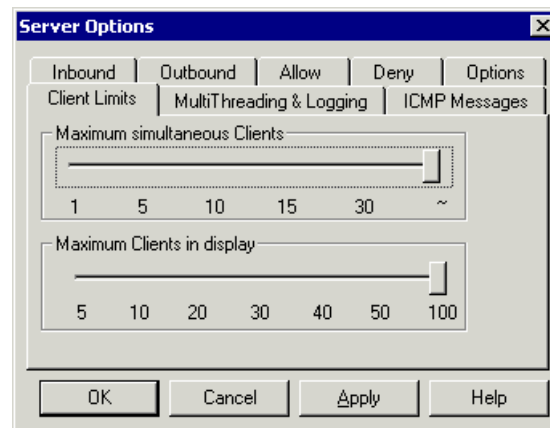
- h. Select the **Deny** tab and ensure that all fields are blank.



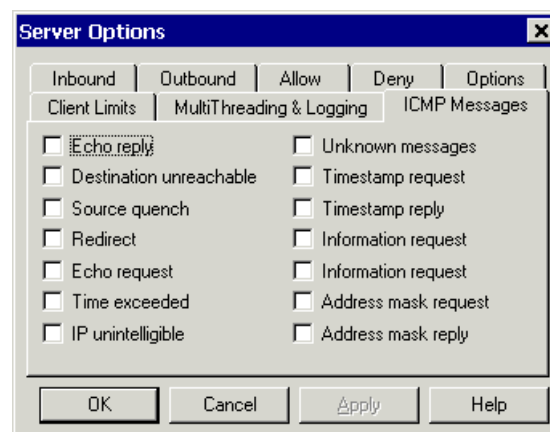
- i. Select the **MultiThreading & Logging** tab and select **High** for **Thread Priority Settings**.
- j. Leave the default filename in the **Log to file** field.



- k. Select the **Client Limits** tab and move the slide button all the way to the right for **Maximum simultaneous Clients** (~) and **Maximum Clients in display** (100).



- l. Select the **ICMP Messages** tab and ensure that all fields are blank.



- m. Click **OK** to save these settings.

This completes the installation and configuration of the TFTP server.

Install the Avaya TFTP server

Index

Numerical

1151A1 and 1151A2 power supply	335
1151A1 power supply	333
1151A2 power supply	333
1151B1/C1 and 1151B2/C2 power supply	334
1152A1 mid-span PDU	324
1152B mid-span PDU	329
120A ICSU	378
2-wire digital station	
connecting	317
pinout chart	318
wiring	317
400B2 Adapter	322
4600 Series IP Telephones	317
46xx IP Phone	
firmware	243 , 621 , 687
46xx IP Phone configuration file.	243 , 621 , 687
808A ETR	319

A

AC power	106
activate pre-upgrade service pack.	571 , 649
adding	
switch configuration	65
adjunct power connections	323
Adjuncts	
connecting	315
alarm wiring	317
analog station	
connecting	317
wiring	317
announcements	347
approved grounds	103
ART, Automatic Registration	
Tool	122 , 251 , 413 , 550 , 630 , 696
ASAI Co-Resident DLG	344
ATM WAN Survivable Processor Manager.	349
Attendant Console, Aux power	323
AUDIX	
IA 770	342
LX	344
Avaya Site Administration	65 , 352
adding new switch configuration	65
configuring	65

B

backup, Linux Migration	572
bonding conductor, install	340
BRI stations	
connecting	318
busy tone disconnect	393

C

C360T-PWR power over Ethernet stackable switch	336
cabling	
multiple units	98
Octaplane Cables	98 , 773
Call Center.	346
G700 announcements	347
CBC	340
CD, Unity	114 , 406
Checklist 1, Install new G700 with S8300	405
checklists	82
Circuit Protection	
Media Modules	341
circuit protection, install	341
CLI commands	67
CO trunk wiring.	317
Command Line Interface Help	62 , 63
Configuration Manager	351
configure	
G700 Media Gateway	446
G700 with S8300	113
administer Communication Manager.	464
completing installation	195 , 489
G700 serial number 117 , 245 , 409 , 544 , 624 , 690	
IP connectivity	451 , 505
LSP transition points	454 , 509
manual procedures.	405
SNMP alarming setup	485
G700 with S8700	201
administer Communication	
Manager	222 , 227 , 519 , 524
completing installation	200 , 240 , 494 , 538
Expansion Module	172 , 220 , 455 , 509
G700 firmware installation	513
tar.gz file	204 , 304 , 498 , 760
TFTP server setup	203 , 303 , 498 , 759
G700 without S8300	
manual procedures.	495

Index

configuring	
Avaya Site Administration	65
switches	65
connect AC power	108
Connecting	
BRI stations	318
connecting a printer to a G700 or G350 Media Gateway.	375
Connecting devices	
BRI stations	318
consoles	
connectable	316
controller list for G700	452 , 506
copy Avaya authentication file	
from computer to server	297 , 667 , 739
copy license file	
from computer to server	297 , 667 , 739
Co-Resident DLG	344
administration tasks.	345
ethernet interfaces	346
coupled bonding conductor, install	340
CWY1 Board	343

D

Data Expansion Modules	72
DC	
wiring diagram	110
DC power	109
default for media gateway	450 , 505
DEFINITY LAN Gateway	344
DHCP server	193 , 484
DID trunk wiring	317
Directory Enabled Management.	350
DLG	344
DS1 loopback jack	376
DS1 span	377
T1	376

E

emergency transfer panel	319
Equipment List	
Avaya Expansion Modules	795
G700	787
Loopback Jack	791
MM710 T1/E1 media module	791
MM711 analog media module	792
MM712 DCP media module	792
MM714 analog media module	792
MM717 DCP media module	792 , 793
MM720 BRI media module	793
MM722 BRI media module	794
MM760 VoIP media module	794

Equipment List, (continued)	
Octaplane Cables	795
Power Cords	788
S8300	789 , 790
X330STK Stacking Sub Module	795
ETR	319
Expansion Module	
G700 with S8700	172 , 220 , 455 , 509
installation	96
external alarm wiring	317
external communications controller (ECC)	394

F

Fault and Performance Manager	351
Firmware upgrades	
configuring in GIW.	149

G

G600 Media Gateway.	80
G650 Media Gateway.	80
G700 Media Gateway	
rack mounting.	89
SNMP alarming setup	485
grounding	
approved	103
conductors	102
connections	105
requirements	102
safety.	105

I

IA770	
language files	561
Initial Administration Tasks	174 , 180 , 465 , 471 , 524
inserting	
Expansion Module.	96
X330STK Stacking Sub-Module	97
installation	
checklists	82
roadmap	112
installing	
telephone power supplies	
procedures	321
Integrated Management.	349
internal communications controller (ICC)	394
Intuity AUDIX	
hunt group	343
IA 770	342
LX	344
IOLAN+ 104 terminal server.	356
installation and administration	356

IP interface
 processor ethernet [187](#), [189](#), [478](#), [532](#)
 IP phone
 configuration file [243](#), [621](#), [687](#)
 firmware [243](#), [621](#), [687](#)
 IP phones
 LSP configuration [193](#), [484](#)
 IP route [448](#), [450](#), [502](#), [505](#)
 IP services [368](#)
 IP Telephone file [274](#), [422](#), [582](#), [651](#), [718](#)
 IP Telephones [317](#)
 ISDN BRI stations
 connecting [318](#)

K

keys.install file [440](#)

L

languages, for IA770 announcements [119](#), [249](#), [265](#), [267](#),
[411](#), [423](#), [548](#), [549](#), [561](#), [583](#), [627](#), [642](#), [645](#), [693](#), [694](#),
[705](#), [719](#)
 laptop
 direct Ethernet connection [172](#), [220](#), [455](#), [509](#)
 LEDs [78](#)
 Linux Migration backup [572](#)
 Local Survivable Processor [80](#)
 Local Survivable Processor screen [179](#), [189](#), [227](#), [470](#), [480](#),
[524](#), [534](#)
 login, super-user [129](#), [255](#), [424](#), [553](#), [596](#), [633](#), [634](#), [698](#),
[732](#)
 loopback jack [376](#)
 administration [378](#)
 installation [376](#)
 LSP [80](#)
 IP phones [193](#), [484](#)
 transition of control [194](#), [485](#)

M

MCC1 Media Gateway [80](#)
 Media Modules [70](#)
 Messaging
 IA770 [342](#)
 LX [344](#)
 MGP controller list [215](#), [452](#), [507](#)
 mid-span power distribution unit [324](#), [329](#)
 MM720 media module
 connecting ISDN BRI stations to [318](#)
 modems, external [391](#)
 administration [392](#)
 hardware to configure [391](#)
 Multi-Tech MT5634ZBA-USB [391](#)
 Multi-Tech MT5634ZBA-V92 [392](#)

multiple units [98](#)
 MultiService SMON Manager [351](#)
 Multi-Tech MT5634ZBA-USB modems [391](#)
 Multi-Tech MT5634ZBA-V92 modems [392](#)
 music-on-hold (MOH) [394](#)

N

network integration [83](#)
 network interface [378](#)
 Network Management Console with
 VoIP SystemView [350](#)

P

P330 LAN Expansion Module [73](#)
 paging equipment [398](#)
 loudspeaker paging for G700 or
 G350 media gateways [398](#)
 pinout chart
 2-wire station [318](#)
 Planning
 documentation [82](#)
 Logins [779](#)
 S8300 Information [783](#)
 Serial Numbers [779](#)
 power
 AC [106](#)
 AC Outlet Test [106](#)
 Connecting [108](#)
 DC [109](#)
 Requirements [106](#)
 Testing the AC Outlet [106](#)
 power supplies
 installation [316](#)
 wiring [316](#)
 power supplies for telephones
 1151A1 -48V [333](#)
 1151A2 -48V [333](#)
 C360T-PWR [336](#)
 installing and wiring [321](#)
 power up [108](#)
 pre-upgrade service pack
 activating [571](#), [649](#)
 printers
 connecting to a G700 or G350 Media Gateway [375](#)
 processor ethernet [179](#), [189](#), [193](#), [227](#), [470](#), [480](#), [524](#), [534](#)
 defining [478](#), [532](#)
 MGP controller list [215](#), [452](#), [453](#), [507](#)
 processor ethernet port [80](#), [484](#), [507](#)
 defining [187](#), [189](#)
 Proxy Agent [351](#)

Index

R

RAL	86
RAM disk	588 , 593 , 724 , 729
disabling	588 , 724
enabling	593 , 729
remaster command	589
Remote Feature Activation	82
Restricted Access Location	86
RJ-45 splitter for connecting two BRI stations	319

S

S8300	
B version	539
LEDs	78
LSP	80
S8300 Media Server	79
S8400 Media Server	80
S8500 Media Server	80
S8700/S8710/S8720 Media Server	80
safety instructions	
1151B1/C1 and 1151B2/C2 power supply	334
SCC1 Media Gateway	80
service pack files	
for Communication Manager	546
Single Sign-On SSO	
RFA Single Sign-On	82
site verification	83
site-specific-option-number (sson)	193 , 484
SNMP alarming on G700	485
stack	448 , 502
stacks	
multiple units	98
super-user login 129 , 255 , 424 , 553 , 596 , 633 , 634 , 698 , 732	
supplementary ground conductor	86
switches	
adding new switch configuration	65
switch-to-call accounting link, testing	373

T

T1 DS1 span	376
task list	112
Technical Specifications Table	773
Telephones	
connecting	315
telephones	
connectable	316
installation	316
wiring	316
telnet	
set parameters	124 , 416 , 577

Terminal Configuration	352
terminal emulation	
ntt	68
w2ktt	68
Terminal Emulator	352
terminal server	356
administering IP services	368
IOLAN+ 104	356
testing, switch-to-call accounting link	373
TFTP server setup	203 , 303 , 498 , 759
translations, CDR parameters	371

U

uninterruptible power supply.	354
Unity CD	114 , 406
upgrade	
existing G700 without S8300	
manual procedures	757
existing S8300A	
manual procedures	539
existing S8300B	
manual procedures	619
existing S8300B or S8300C	
manual procedures	685
G700 with S8300	241
completing upgrade (S8300 primary controller)	298 , 617 , 681 , 753
configure G700 Media Gateway	668 , 740
G700 with S8400	301
G700 with S8500	301
G700 with S8700	301
G700 firmware installation	765
Upgrade Tool	
upgrading a G700	301
UPS	354
USB CD-ROM drive	114 , 406

V

Voice Announcement over LAN Manager	353

W

wiring	
2-wire digital station	317
alarm	317
analog station	317
CO trunk	317
DID trunk	317
wiring diagram	
DC	110
wiring telephone power supplies	
procedures	321

X

X330 WAN Access Routing Module	73
X330STK Stacking Sub-Module	
installation	97

