Installation and Upgrades
for **Avaya G700 Media Gateway** and
Avaya S8300 Media Server

555-234-100
Issue 8.1
June 2005

Copyright 2005, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

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.

Preventing Toll Fraud

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

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya 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.

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997, EN55022:1998, and AS/NZS 3548.

Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

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

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

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

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

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

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

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

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

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

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Installation and Repairs

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

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier’s Declaration of Conformity (SDoC)

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

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

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

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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

Japan

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

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

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support 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 33
Downloading this book 33
Safety labels and security alert labels 34
Related resources 34
Technical assistance 35
Within the United States. 35
International 35
Trademarks. 36
Ordering Documentation 36
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 the Avaya Installation Wizard (IW) 42
What the IW Does and Does Not Do 43
Electronic Worksheets and Templates 44
About the Upgrade Tool 45
You cannot use the Upgrade Tool to: 45
About the Avaya Gateway Installation Wizard 46
About connection and login methods 47
What physical access methods are available 47
Laptop configuration for direct connection to the services port 48
What network settings are required on the laptop 49

Configuring the laptop for a direct connection 49
About connection methods 54
Connecting a laptop to services port of S8300 54
Connecting a laptop to the G700 serial port 54
Connecting a laptop to the customer LAN 55
Connecting an external modem to the S8300 media server 55
Setting up Windows for modem connection to the media server (Windows 2000 or XP) 56
Configuring the Remote PC for PPP Modem Connection (Windows 2000 or XP, Terminal Emulator, or ASA) 57
Using Windows for PPP Modem Connection (Windows 2000 or XP) . . . 58
Using Avaya Terminal Emulator for LAN Connection to Communication Manager 59
Using Avaya Terminal Emulator for Modem Connection to Communication Manager 60
About Log in Methods 61
Logging in to the media server from your laptop using Telnet 61
Logging in to the S8300 Web Interface from your Laptop 62
Open the Communication Manager SAT Screens 66
Logging in to the P330 Stack Processor with a Direct Connection to the S8300 Services Port 66
Logging in to the P330 Stack Processor with a LAN Connection 67
Logging in to the P330 Stack Processor with a Direct Serial Connection . 68
Logging in to the P330 Stack Processor with Device Manager 68
About Avaya Site Administration 69
Configuring Avaya Site Administration 69
About navigation for G700 CLI commands 71
About terminal emulation function keys for Communication Manager 73

Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server. 75
About hardware components 75
What are the main elements of the G700 media gateway 75
What comprises the G700 media gateway chassis and processors 76
What are the media modules 76
What are data expansion modules 78
What are stackable ethernet switches 79
What are the functions of the S8300 LED Indicators 81
Media servers supporting the G700 media gateway 82
What is the S8300 media server 82
What is the S8500 media server 83

What is the S8700/S8710 media server 83
About endpoint and adjunct components 83
About installation planning 84
What the planning documentation provides 84
Who needs a Single Sign-On (SSO) authentication login 85
What site verification does 85
What network integration requires 85
About installation and cabling 86
Verifying the on-site checklist 86
Verifying Environmental conditions 87
Power Verification 87
Grounding Verification 87
Unpacking and checking the order 88
Installing the G700 media gateway 88
Preparing the G700 media gateway 89
Mounting the G700 media gateway in the rack 90
Inserting the Avaya S8300 media server (if necessary for standalone service or LSP) 92
Inserting media modules 94
Inserting an Expansion Module 97
Inserting an Avaya X330STK Stacking Module 98
Cabling multiple units 99
Attaching Ground Conductors 103
What are general grounding requirements 103
What are approved grounds 104
Connecting the Safety Ground 106
Connecting AC Power 107
What are the G700 AC power requirements 107
Testing the AC Outlet 107
Plugging in AC power 109
Checking and Connecting DC Power 110

Section 2: G700 installation and upgrades - wizards 113

About the Installation Roadmap and Task Lists 114
Checklist 1: Install a New G700 with an S8300 (Primary or LSP) 114
Checklist 2: Install a New G700 without an S8300 117

Checklist 3
Upgrade an Existing G700 with an S8300A to R3.0 119
Checklist 4
Upgrade an Existing G700 with an S8300B to R3.0 121
Checklist 5:
Upgrade an Existing G700 without an S8300 123

Chapter 3: Installing a new G700 with an S8300 125
Installation Overview 126
About G700 components 126
About software and firmware files 126
About access to the Server CD 127
System Access. 128
What provides initial access to the G700 128
How is normal access to the S8300 and G700 provided 128
Connecting directly to a target S8300 128
Connecting directly to the remote primary server (S8300, S8500, or S8700). 129
Connecting using the customer's LAN. 129
Before Going to the Customer Site. 130
Installing TFTP server (or obtaining USB CD-ROM drive) 130
Collecting Installation Information 131
Planning forms provided by the Project Manager 131
Getting the Serial Number of the G700, if Necessary. 131
Checking the FTP Server for Backing up Data. 131
Obtaining service pack files, if needed. 132
If using IA770, obtaining service pack and language files 133
Obtaining an IA770 service pack file 133
Obtaining Optional language files 134
Obtaining Ethernet interface IP address and subnet mask 134
Completing the RFA process (Obtaining license and password file) 134
Install the S8300 137
Inserting the S8300 137
Installing Communication Manager Software 138
Setting telnet parameters 138
Remastering the hard drive and installing the software 138

About the Avaya Installation Wizard 144
Configure the S8300 Media Server 144
Enabling Network Time Servers 145
Configure the G700 Media Gateway 146
Install new firmware on the G700 146
Electronic worksheets and templates 147
Electronic pre-installation worksheet 147
Name and number list (S8300 with G700 or G350 only) 147
Custom template (S8300 with G700 or G350 only) 148
Obtaining further information on the Avaya Installation Wizard 148
Using the Avaya Installation Wizard (IW) 148
Installing IA770 service pack files, if any 157
Configuring an X330 Expansion Module (if necessary) 158
Setting rapid spanning tree on the network 159
Administer Communication Manager 160
Administering an S8300 primary controller 160
Assigning Node Names and IP Addresses for the LSPs 161
Administering Network Regions 162
Associating LSPs with Network Regions 163
Administering IP Interfaces 164
Administering the LSP Form 164
Administering an S8500 or S8700 primary controller 166
Assigning Node Names and IP Addresses for the C-LANs and LSPs . . . 167
Administering Network Regions 167
Assigning LSPs to the Network Regions 170
Administering IP Interfaces 170
Administering the LSP Form 172
Administering the Media Gateway 173
Considerations for IP Phones Supported by a Local Survivable Processor . . . 177
Transition of Control from Primary Controller to LSP 178
Complete the Installation of the S8300 (if the Primary Controller) 179
Backing up the system 179
If using IA770, administer Communication Manager for Integrated Messaging . . 180
Complete the Installation Process (for an S8300 LSP) 181

Chapter 4: Installing a new G700 without an S8300 183
Installation overview. 184
What are the system components 184
About G700 components 184
About firmware files 184
About the TFTP server. 184
What provides initial access to the G700 184
How is normal access to the S8300 and G700 provided 185
Connecting directly to a target S8300 185
Connecting directly to the remote primary server (S8300, S8500, or S8700). 185
Connecting using the customer's LAN. 186
Before going to the customer site 187
Collecting Installation Information 187
Planning forms that the Project Manager provides 187
Getting the Serial Number of the G700, if Necessary. 187
Installing the Gateway Installation Wizard 188
Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary. 188
Downloading G700 firmware files to your TFTP directory 189
Downloading individual firmware files 189
Configure the G700 190
Install firmware on the G700 and media modules 191
Configure an X330 Expansion Module (If Necessary) 191
Set rapid spanning tree on the network 192
Administer Communication Manager 193
Administering an S8300 primary controller 193
Assigning Node Names and IP Addresses for the LSPs 194
Administering Network Regions 194
Associating LSPs with Network Regions 196
Administering IP Interfaces 196
Administering the LSP Form 197
Administering an S8500 or S8700-series primary controller 198
Assigning Node Names and IP Addresses for the C-LANs and LSPs . . . 199
Administering Network Regions 200
Assigning LSPs to the Network Regions. 202
Administering IP Interfaces 203
Administering the LSP Form 204
Administering the Media Gateway 205
Complete the Installation Process 209

Chapter 5: Upgrading an existing S8300A to R3.0 using the Wizards . 211
About upgrading an existing S8300A to R3.0 211
Release 3.0 upgrade scenarios 212
Accessing the Server CD 213
Accessing the S8300 214
Before going to the customer site 214
Installing TFTP server or obtaining USB CD-ROM drive 215
Collecting upgrade information. 215
Filling in the EPW, if upgrading from release 1.1 215
Planning forms provided by the project manager 215
Getting the serial number of the G700, if necessary 216
Checking the number of allocated ports 216
Identifying the FTP server for backing up data 216
Obtaining S8300 software and G700 firmware. 217
Obtaining service pack files 218
If using IA770, checking stored messages size, obtaining service pack (or RFU) and language files 219
Checking the size of stored messages. 220
Obtaining an IA770 service pack file 220
Obtaining optional language files 221
Completing the RFA process (obtaining license and authentication files) 221
Preparing for the upgrade on-site 224
Accessing the S8300 224
Checking current software release 225
Pre-Upgrade Tasks — If the S8300 is the primary controller 226
Getting IA770 data and stopping IA770 (if IA770 is being used). 230
Creating an IA770 test message 230
Determining whether optional languages are needed. 230
Stopping IA770. 233
Backing up system files. 233
Recording configuration information 236
Upgrading the S8300A. 237
Installing the pre-upgrade software service pack, if necessary 238
Installing the pre-upgrade service pack 238
Linux migration backup (if current release is 1.2.0 through 1.3.x) 240
Replacing the S8300A with the S8300B Media Server 243

Upgrading Communication Manager software 244
Setting telnet parameters 245
Remastering the hard drive and installing the upgrade software 245
Verifying software version 251
Copying files to the S8300 252
Configuring network parameters 254
Verifying connectivity 255
Installing post-upgrade Communication Manager service pack file from your laptop 256
Restoring data 257
Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) 257
Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x) 258
Verifying the time, date, and time zone. 262
Verifying media server configuration. 262
Installing the updated license file 264
Installing the new authentication file, if any 265
Saving translations (if not using IA770 and S8300 is not an LSP) 266
Verifying operation 266
Next steps 267
Upgrade the firmware on the G700 Media Gateway 268
Upgrading the G700 using the Installation Wizard 268
Upgrading the G700 using the Upgrade Tool 269
Setting rapid spanning tree on the network 269
Post-upgrade tasks 270
If using IA770: 271
Restore AUDIX data 271
Saving translations 276
Installing IA770 service pack (or RFU) files and optional language files, if any 276
Complete the upgrade process (S8300 is the primary controller) 277

Chapter 6: Upgrading an existing S8300B to R3.0 using the Wizards . 279
About upgrading the S8300B to release 3.0 and upgrading G700 firmware 279
Major tasks to upgrade the S8300B to release 3.0 and upgrade the G700 firmware 280

Before going to the customer site 280
Planning forms provided by the project manager 281
Getting the serial number of the G700, if necessary 281
Checking the number of allocated ports 281
Checking the FTP server for backing up data 281
Obtaining S8300 software and G700 firmware 282
Obtaining service pack files 282
Pre-upgrade service pack 282
Obtaining service pack and language files, if using IA770 284
Checking for IA770 stored messages size 284
Obtaining an IA770 service pack file 285
Obtaining optional language files 285
Completing the RFA process (obtaining license and password file). 285
On-site Preparation for the Upgrade 288
Accessing the S8300 288
Completing pre-upgrade tasks — If the target S8300 is the primary controller 289
Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used) 292
Determining whether optional languages are needed. 292
Downloading optional language files, if needed. 294
Creating an IA770 test message for the upgrade 295
Shutting down IA770. 295
Backing up S8300 recovery system files. 296
Copying the service pack files to the media server 298
Installing the pre-upgrade software service pack 299
Copying license and authentication files to the S8300 hard drive (from your laptop) 300
Copying the software and firmware files from the Server CD 302
Upgrade the S8300. 307
Upgrading the S8300B using the Web Interface 307
Installing new software 307
Making the upgrade permanent. 311
Installing post-upgrade Communication Manager service pack, if any 311
Install updated license and authentication files 312
Saving translations (only if new license and/or authentication files installed) 313
Upgrade the G700 Firmware 314
Upgrading G700 firmware using the installation wizard 314
Upgrading G700 firmware using the upgrade tool from the primary controller 318
Setting rapid spanning tree on the network 318

Post-upgrade tasks 319
Installing IA770 service pack (or RFU) files, if any 319
Completing the upgrade process (S8300 is the primary controller) 320

Chapter 7: Upgrading an existing G700 without an S8300 323
About the existing G700 upgrade. 323
What are the G700 system components 323
About firmware files 324
About the TFTP server. 324
About system access 324
Accessing the G700 324
Before going to the customer site 325
Planning forms that the project manager provides 325
Getting the serial number of the G700, if necessary 325
Setting up the TFTP server on your laptop or on a customer PC, if necessary 326
Downloading G700 firmware files to your TFTP directory 326
Downloading individual firmware files 326
On-site preparation for the upgrade 328
Accessing the P330 Stack Processor 328
Verifying the contents of the tftpboot directory 329
Determining which firmware to install on the G700 329
Installing new firmware on the G700 Media Gateway 331
Setting rapid spanning tree on the network 332

Chapter 8: Telephones and adjunct systems 333
Installation and wiring of telephones and power supplies 334
About connectable telephones and consoles 334
Connecting telephones 335
Connecting an analog station or 2-wire digital station 335
Connecting an ISDN BRI station to an MM720 Media Module 337
Installing an 808A Emergency Transfer Panel and associated telephones 338
Installing and wiring telephone power supplies 339
1152A1 mid-span power distribution unit 343
Connecting the 1152A1 PDU cables 345

1151B1 and 1151B2 power supplies 347
Important safety instructions for 1151B1 and 1151B2 power supplies 347
Using the 1151B1 and 1151B2 power supplies 348
Connecting the 1151B1 or 1151B2 power supplies 349
Avaya Power over Ethernet (PoE) switches 349
Available PoE Switch Options 349
Power priority mechanism 350
C360 converged stackable switches 351
Features of the C360 converged stackable switches 352
C460 converged multi-layer switch. 355
P333T-PWR power over ethernet stackable switch 356
Important P333T-PWR switch safety instructions 357
Using the P333T-PWR switch 357
Connecting the P333T-PWR switch. 358
Complete the telephone installation process 360
Installing the coupled bonding conductor 360
Installing over-voltage and sneak-current circuit protection 361
IA 770 INTUITY AUDIX messaging application 362
Shared resources of IA770 coresidency 362
Where is the IA770 location and software 363
Using an AUDIX trunk group as well as an AUDIX hunt group for new systems 363
IA 770 INTUITY AUDIX installations and S8300 upgrades for IA 770 INTUITY AUDIX 363
INTUITY AUDIX LX messaging system 364
ASAI co-resident DEFINITY LAN gateway (DLG) 364
PROCR administration task summary (for the S8300 Media Server) 365
Supported Ethernet Interfaces 366
Call center 366
About Avaya G700 announcement software 367
Avaya Integrated Management 369
Avaya ATM WAN Survivable Processor Manager 369
Avaya Directory Enabled Management 370
Avaya MultiService Network Manager 370
Avaya MultiService SMON Manager 371
Avaya Fault and Performance Manager 371
Avaya Proxy Agent 371
Avaya Configuration Manager 371

Avaya Site Administration 372
Avaya Terminal Configuration 372
Avaya Terminal Emulator 372
Avaya Voice Announcement Over LAN Manager 373
Avaya VoIP Monitoring Manager 373
Uninterruptible power supply (UPS) 374
Terminal server installation 376
Installing and administering the terminal server 376
What are the distance limits for the terminal server. 377
How is the terminal server cabling connected. 378
Connecting the IOLAN+ to the adjunct and the LAN 378
Administering the IOLAN+ 379
Navigating the IOLAN+ terminal server 383
Administering the gateway 384
Administering an IOLAN+ port 384
Testing connectivity through the IOLAN+ 386
Potential failure scenarios and repair actions 388
Administering IP services 388
Call detail recording (CDR) 390
Connecting CDR equipment 390
Administering CDR data collection. 390
Administering CDR parameters. 391
Testing the switch-to-adjunct link 393
Reliable Data Transport Tool (RDTT) package 394
What does the RDTT package contain 394
Downloading the RDTT package 394
Installing the RDTT package 395
Administering the RDTT package 395
Related topics 395
Printers 395
DS1/T1 CPE loopback jack 396
Installing a loopback jack 396
Installing a loopback jack with a smart jack 396
Installing a loopback jack without a smart jack 397
Administering a loopback jack 398
Testing a loopback jack with a smart jack 398
Testing the DS1 span from the ICSU to the loopback jack 398
Checking the integrity of local equipment 399
Testing the integrity of data sent over the loop 400

Testing the DS1 span from the smart jack to the network interface termination or fiber multiplexer (MUX) 403
Testing the DS1 span from the loopback jack to the smart jack 403
Testing a loopback jack without a smart jack 407
Configurations using fiber multiplexers 410
Checking for the presence of DC 410
External modems 411
Hardware required when configuring modems 411
Multi-Tech MT5634ZBA-USB-V92 411
Configuring the MT5634ZBA-USB-V92 modem 412
Multi-Tech MT5634ZBA-V92-GLOBAL 412
Administering Multi-Tech modems 412
Busy tone disconnect equipment for non-U.S. installations 413
Music-on-hold 414
Installing an unregistered music source on a G700 or G350 Media Gateway . 414
Installing a registered music source on a G700 or G350 Media Gateway . . . 417
Paging and announcement equipment 418
Adjunct Information Sources 419
Call Management System 419
INTUITY AUDIX Messaging Systems 420
Avaya Modular Messaging System 420
ASAI and DEFINITY LAN Gateway 420
Avaya Interactive Response 420
Avaya EC500 Extension to Cellular and Off-PBX Stations 421
Converged Communications Server 421
Seamless Converged Communications across Networks (SCCAN) 421
Call Accounting Systems 421

Section 3: G700 installation and upgrades - manual procedures . . 423
About the Installation Roadmap and Task Lists 424
Checklist 1: Install a new G700 with an S8300 (Primary or LSP) 424
Checklist 2: Install a new G700 without an S8300 427
Checklist 3 Upgrade an existing G700 with an S8300A to R3.0 429

Checklist 4
Upgrade an existing G700 with an S8300B to R3.0 431
Checklist 5:
Upgrade an existing G700 without an S8300 433

Chapter 9: Manual installation of a new G700 with an S8300 435
Installation Overview 436
About G700 components 436
About software and firmware files 436
About access to the Server CD 436
System Access. 437
What provides initial access to the G700 437
How is normal access to the S8300 and G700 provided 437
Connecting directly to a target S8300 438
Connecting directly to the remote primary server (S8300, S8500, or S8700). 438
Connecting using the customer's LAN. 439
Before Going to the Customer Site. 439
Upgrading to release 3.0 (Install TFTP server or obtain USB CD-ROM drive) 440
Collecting Upgrade Information 440
Planning Forms that the Project Manager provides. 440
Getting the Serial Number of the G700, if Necessary. 441
Checking the FTP Server for Backing up Data. 441
Obtaining service pack files, if needed. 441
If using IA770, obtaining service pack and language files 442
Obtaining an IA770 service pack file 443
Obtaining Optional language files 443
If using IA770, obtain Ethernet interface IP address and subnet mask 443
Completing the RFA process (Obtaining license and password file) 443
Install the S8300 446
Inserting the S8300 446
Installing Communication Manager Software 446
Setting telnet parameters 446
Remastering the hard drive and installing the software 447
Verifying Software Version 453
Copying Files to the S8300 hard drive 454

Verifying the Time, Date, and Time Zone 456
Installing License and Authentication Files 456
Saving Translations 458
Installing Communication Manager service pack files, if any 458
Configuring the S8300 459
Providing the keys.install File (If Necessary) 473
Setting the media server's time 475
If using IA770, install messaging software 475
Configure the G700 Media Gateway 476
Assigning IP Addresses of the G700 Media Gateway Components 476
Checking for IP connections 481
Setting up the Controller List for the G700 482
Setting the LSP Transition Points 484
Configuring an X330 Expansion Module (If Necessary) 484
Install New Firmware on the G700 485
Manual upgrade procedures — G700 firmware 485
Verifying the Contents of the tftpboot Directory 485
Determining which firmware to install on the G700 486
Installing New Firmware on the P330 Stack Processor 488
Installing new firmware on the G700 Media Gateway Processor 488
Installing new firmware on the media modules 490
Setting rapid spanning tree on the network 492
Installing IA770 service pack files, if any 493
Administer Communication Manager 494
Administering an S8300 primary controller 494
Assigning Node Names and IP Addresses for the LSPs 495
Administering Network Regions 496
Associating LSPs with Network Regions 497
Administering IP Interfaces 498
Administering the LSP Form 498
Administering an S8500 or S8700 primary controller 499
Assigning Node Names and IP Addresses for the C-LANs and LSPs . . . 500
Administering Network Regions 501
Assigning LSPs to the Network Regions 503
Administering IP Interfaces 504
Administering the LSP Form 505
Administering the Media Gateway 506
Considerations for IP Phones Supported by a Local Survivable Processor . . . 510
Transition of Control from Primary Controller to LSP 511

Set Up SNMP Alarming on the G700 511
Configuring the primary server to report alarms to a services support agency 512
Administering INADS phone numbers and Enabling alarms to INADS . . 512
Configuring the G700 Media Gateway to send its traps to a network management system (NMS). 513
Configuring an SNMP community string for traps 513
Configuring the destination for G700 SNMP traps 514
Complete the Installation of the S8300 (if the Primary Controller) 515
Backing up the system 515
If using IA770, administer Communication Manager for Integrated Messaging. . 516
Complete the Installation Process (for an S8300 LSP) 517

Chapter 10: Manual installation of a new G700 without an S8300 . . . 519
Installation overview. 520
What are the system components 520
About G700 components 520
About firmware files 520
About the TFTP server. 520
What provides initial access to the G700 520
How is normal access to the S8300 and G700 provided 521
Connecting directly to a target S8300 521
Connecting directly to the remote primary server (S8300, S8500, or S8700). 522
Connecting using the customer's LAN. 522
Before going to the customer site 523
Collecting Installation Information 523
Planning forms that the Project Manager provides 523
Getting the Serial Number of the G700, if Necessary. 524
Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary. 524
Downloading G700 firmware files to your TFTP directory 524
Downloading individual firmware files 525
Configure the G700 526
Assigning the IP addresses of the G700 media gateway components 526
Checking for IP connections 531
Setting up the controller list for the G700 532
Setting the LSP Transition Points 534
Configuring an X330 Expansion Module (If Necessary) 535

Prepare to install firmware on the G700 536
Accessing the P330 Stack Processor 536
Verifying the contents of the tftpboot directory 536
Determining which firmware to install on the G700 537
Install New Firmware on the G700 Media Gateway 539
Manually installing G700 and media modules firmware 539
Installing New Firmware on the P330 Stack Processor 539
Installing new firmware on the G700 Media Gateway Processor 540
Installing new firmware on the media modules 541
Setting rapid spanning tree on the network 543
Administer Communication Manager 544
Administering an S8300 primary controller 545
Assigning Node Names and IP Addresses for the LSPs 545
Administering Network Regions 546
Associating LSPs with Network Regions 547
Administering IP Interfaces 548
Administering the LSP Form 549
Administering an S8500 or S8700/S8710 primary controller 550
Assigning Node Names and IP Addresses for the C-LANs and LSPs . . . 551
Administering Network Regions 552
Assigning LSPs to the Network Regions. 554
Administering IP Interfaces 555
Administering the LSP Form 556
Administering the Media Gateway 557
Complete the Installation Process 561

Chapter 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware 563
About upgrading an existing S8300A to R3.0 563
Release 3.0 upgrade scenarios 564
Accessing the Server CD 565
Accessing the S8300 566
Before going to the customer site 566
Installing TFTP server or obtaining USB CD-ROM drive 567
Collecting upgrade information. 567
Filling in the EPW, if upgrading from release 1.1 567
Planning forms provided by the project manager 567
Getting the serial number of the G700, if necessary 568

Checking the number of allocated ports 568
Identifying the FTP server for backing up data 568
Obtaining S8300 software and G700 firmware 569
Obtaining service pack files, if needed 570
If using IA770, checking stored messages size, obtaining service pack (or RFU) and language files 571
Checking the size of stored messages 572
Obtaining an IA770 service pack file 572
Obtaining optional language files 573
Completing the RFA process (obtaining license and authentication files) 573
Preparing for the upgrade to R3.0 on-site 576
Accessing the S8300 576
Checking current software release 577
Pre-Upgrade Tasks — If the S8300 is the primary controller 578
Getting IA770 data and stopping IA770 (if IA770 is being used) 582
Creating an IA770 test message 582
Determining whether optional languages are needed 582
Stopping IA770 584
Backing up system files 585
Recording configuration information 588
Upgrading the S8300A 589
Installing the pre-upgrade software service pack, if necessary 589
Installing the pre-upgrade service pack 590
Linux migration backup (if current release is 1.2.0 through 1.3.x) 592
Replacing the S8300A with the S8300B Media Server 595
Upgrading the S8300B Media Server 596
Setting telnet parameters 596
Remastering the hard drive and installing the upgrade software 597
Verifying software version 602
Copying files to the S8300 603
Configuring network parameters 605
Verifying connectivity 606
Installing post-upgrade Communication Manager service pack file from your laptop 607
Restoring data 608
Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) 608

Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x) . . . 609
Verifying the time, date, and time zone. . . . 613
Verifying media server configuration. . . . 613
Installing the new license file . . . 615
Installing the new authentication file, if any . . . 616
Saving translations (if not using IA770 and S8300 is not an LSP) . . . 617
Verifying operation . . . 617
Next steps . . . 618
Upgrade the firmware on the G700 Media Gateway . . . 619
Manually upgrading G700 firmware . . . 619
Verifying the contents of the tftpboot directory . . . 619
Determining which firmware to install on the G700 . . . 620
Installing new firmware on the P330 Stack Processor . . . 622
Installing new firmware on the G700 Media Gateway Processor . . . 622
Installing new firmware on the media modules . . . 624
Setting rapid spanning tree on the network . . . 626
Installing new firmware on other G700 media gateways . . . 627
Post-upgrade tasks . . . 628
If using IA770: . . . 629
Install and restart IA770 . . . 629
Saving translations . . . 635
Installing IA770 service pack (or RFU) files and optional language files, if any . . . 635
Complete the upgrade process (S8300 is the primary controller) . . . 636

Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware . . . 639
About upgrading the S8300B to release 3.0 and upgrading G700 firmware . . . 639
Major tasks to upgrade the S8300B to release 3.0 and upgrade the G700 firmware . . . 640
Before going to the customer site . . . 640
Planning forms that the project manager provides . . . 641
Getting the serial number of the G700, if necessary . . . 641
Checking the number of allocated ports . . . 641
Checking the FTP server for backing up data . . . 641
Obtaining S8300 software and G700 firmware . . . 642
Obtaining service pack files . . . 642
Pre-upgrade service pack . . . 642

Obtaining service pack and language files, if using IA770 644
Checking for IA770 stored messages size 644
Obtaining an IA770 service pack file 645
Obtaining optional language files 645
Completing the RFA process (obtaining license and password file). 645
On-site Preparation for the Upgrade 648
Accessing the S8300 648
Completing pre-upgrade tasks — If the target S8300 is the primary controller 649
Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used) 652
Determining whether optional languages are needed. 652
Downloading optional language files, if needed. 654
Creating an IA770 test message for the upgrade 655
Shutting down IA770. 655
Backing up S8300 recovery system files. 656
Installing the pre-upgrade software service pack 658
Copying license and authentication files to the S8300 hard drive (from your laptop) 659
Copying the software and firmware files from the Server CD 661
Upgrade the S8300. 666
Manually upgrading the S8300 666
Installing new software 666
Making the upgrade permanent. 670
Installing post-upgrade Communication Manager service pack file from your laptop, if any 671
Install updated license and authentication files 672
Saving translations (only if new license and/or authentication files installed) 673
Upgrade the G700 Firmware 674
Manually upgrading G700 firmware 674
Verifying the contents of the tftpboot directory 674
Determining which firmware to install on the G700 675
Installing new firmware on the P330 stack processor. 677
Installing new firmware on the G700 Media Gateway Processor 677
Installing new firmware on the media modules 679
Setting rapid spanning tree on the network 681
Installing new firmware on other G700 media gateways 682
Post-upgrade tasks 683
Installing IA770 service pack (or RFU) files, if any 683
Completing the upgrade process (S8300 is the primary controller) 684

Chapter 13: Manual upgrade of an existing G700 without an S8300 687
About the existing G700 upgrade. 687
What are the G700 system components 687
About firmware files 688
About the TFTP server. 688
About system access 688
Accessing the G700 688
Before going to the customer site 689
Planning forms that the project manager provides 689
Getting the serial number of the G700, if necessary 689
Setting up the TFTP server on your laptop or on a customer PC, if necessary 690
Downloading G700 firmware files to your TFTP directory 690
Downloading individual firmware files 690
On-site preparation for the upgrade 692
Accessing the P330 stack processor. 692
Verifying the contents of the tftpboot directory 692
Determining which firmware to install on the G700 693
Install new firmware on the G700 Media Gateway 695
Manually installing G700 and media modules firmware 695
Installing new firmware on the P330 stack processor. 696
Installing new firmware on the G700 Media Gateway Processor 696
Installing new firmware on the media modules 698
Setting rapid spanning tree on the network 700

Appendix A: Technical information 701
Avaya G700 Media Gateway Technical Specifications 701
Cabling Equipment 702

Appendix B: Information checklists 705
Installer's Checklist 706
Serial Number and Login Information 707
G700 Serial Numbers 707
Logins 707
Set-Up for P330 Stack Processor 708
Set Up for G700 Media Gateway Processor (MGP) 709
Set Up for VoiP Resources 710

Set Up for S8300 Media Server 711
Installation Site Information. 713
Stack Layout 714

Appendix C: Equipment list. 715

Appendix D: Install the Avaya TFTP server 725

Index 731

About this book

Overview

This document provides procedures to install, upgrade, or add to an Avaya G700 Media Gateway controlled by an Avaya S8300, S8500, or S8700/S8710 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

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
- Chapter 4: Installing a new G700 without an S8300
- Chapter 5: Upgrading an existing S8300A to R3.0 using the Wizards
- Chapter 6: Upgrading an existing S8300B to R3.0 using the Wizards
- Chapter 7: Upgrading an existing G700 without an S8300

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 8: 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 9: Manual installation of a new G700 with an S8300
- Chapter 10: Manual installation of a new G700 without an S8300
- Chapter 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware
- Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware
- Chapter 13: Manual upgrade of an existing G700 without an S8300

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 8: 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 *Installation and Upgrades for 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.

Downloading this book

To download the latest version of this book:

1. Access the Avaya web site at http://support.avaya.com.
2. On the left side of the page, click **Product Documentation**.
3. The system displays the Welcome to Product Documentation page.
4. On the right side of the page, type **555-234-100**, and then click **Search**.
5. The system displays the Product Documentation Search Results page.
6. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
7. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book in zipped PDF format

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 June 2004 release of Avaya Communication Manager, see *Highlights of Avaya Communication Manager*, 555-245-704.

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

Title	Number
Overview for Avaya G700 Media Gateway and Avaya S8300 Media Server	555-234-200
Maintenance Commands Reference	555-245-101
Maintenance Alarms Reference	555-245-102
Maintenance Procedures	555-245-103
Quick Start: Avaya G700 Media Gateway Hardware Installation	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, *Installation and Upgrades for Avaya G700 Media Gateway and Avaya S8300,* 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, three 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.

  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 wizards, as well as wizard Job Aids at http://support.avaya.com/avayaiw.

Tip:

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

When to use each wizard

Table 1 shows at-a-glance when you would use each tool. For more detailed information on choosing the right wizard, see *Job Aid: What Provisioning Tools and Wizards Should I Use?,* 555-245-755.

Table Legend:

IW= Avaya Installation Wizard
UT = Upgrade Tool
GIW = Gateway Installation Wizard).

Table 1: When to use each wizard

Component	Use	New Installation	Upgrade Software	Upgrade Firmware
S8500 or S8700/ S8710	as a Primary Controller	IW	IW	
S8300	as an LSP	IW	IW, UT*	
	as a Primary Controller	IW	IW	
G350 or G700	with an S8300	IW		IW, UT†
	without an S8300	GIW		UT

*. Use the UT to schedule upgrades of multiple LSPs. Use the IW on site for an immediate upgrade of a single LSP.

†. Use UT to schedule upgrades of multiple gateways. Use the IW on site for an immediate upgrade of a single gateway or G700 stack.

Table 2 summarizes when you would use each tool and what it does for you.

Table 2: What each wizard does for you

If you need to:	Then use:
Install new or upgrade existing S8300, S8500 or S8700/S8710 Media Servers, including: • The G350 or G700 that contains an S8300 • Other G700s in the stack • G350/G700 media modules	The ***Avaya Installation Wizard*** (IW) on site, with a laptop connection to the Services port on the media server. **NOTE:** Since the source files for an upgrade are large, the IW requires that these source files be accessible (to the media server running the IW) over a high-bandwidth connection. The files could be on the media server's hard drive (ftp/pub directory), on a CD-ROM drive connected to the media server, or on the CD-ROM drive or hard drive on a technician's laptop directly connected to the media server. If the source files are available on one of these media, you could use the IW from a remote location using a dialup PPP connection to the media server (with modem enabled) running the IW. This wizard installs new (or upgrades existing) software on media servers and performs the initial configuration. It upgrades firmware on new or existing media gateway processors and media modules. You will also use the Electronic Pre-installation Worksheet, which you get from your project manager. For the S8300/G700, you may also use the Name and Number List and the Custom Template with the wizard for more comprehensive custom installations.

1 of 2

Table 2: What each wizard does for you (continued)

If you need to:	Then use:
Install a new G350 or G700 that does not contain an S8300	The ***Gateway Installation Wizard*** (GIW) on site, with a laptop connection to the G350 or G700. This wizard configures the IP addresses for the gateway, including the gateway processors, the controller list, and the VoIP engine. The GIW does not install firmware on the G350 or G700 or their media modules. You can install firmware manually, or use the UT.
Schedule upgrades of multiple, geographically-distributed LSPs or G350/G700 gateways, all of which have the same remote primary controller — S8300, S8500, or S8700/S8710	The ***Upgrade Tool*** (UT), running on the primary controller, using a remote network connection. This tool enables you to upgrade: ● the software on all LSPs registered with the primary controller ● the processor and media module firmware for all gateways currently or previously registered with the primary controller. **NOTE:** If the customer has purchased and installed the MultiService Software Update Manager, you may wish to use it, instead, to upgrade G350 or G700 Media Gateways. However, the Software Update Manager cannot upgrade LSPs.

2 of 2

About the Avaya Installation Wizard (IW)

You can use the Avaya Installation Wizard (IW) as a tool to assist you in the installation and upgrade processes for S8300, S8500, and S8700/S8710 Media Servers, and G350 and G700 Media Gateways. The Installation Wizard is designed to get you up and running in a basic installation as quickly as possible. For customized installations, optional custom templates are also available.

The Avaya Installation Wizard ships with the media server software and is accessible on the home page of the Integrated Management web interface. The most recent version of IW, as well as its documentation, can be accessed online at http://support.avaya.com/avayaiw, or see the document *Job Aid: Avaya Installation Wizard,* 555-245-754.

Note:

To use the IW, Communication Manager Release 2.0 or later must be running on the media server (S8300, S8500, or S8700/S8710). If the correct release of Communication Manager has not been installed on the media server, you need to upgrade the software before you begin using the IW.

What the IW Does and Does Not Do

The IW automates many but not all tasks in an S8300 Media Server installation.

Tasks IW automates

Of the tasks in Chapter 3, Installing a New G700 with an S8300, the IW automates the following:

- Installing Communication Manager service pack files, if any
- Configuring the S8300

  Note:

  See Using the Avaya Installation Wizard (IW) on page 148
- Configure the G700 Media Gateway
- Install new firmware on the G700

  Note:

  In addition, you can use the IW to upgrade media server software or gateway firmware on a previously-installed system.

The IW automates similar tasks in Chapters 4–6.

Tasks IW does not automate

You must perform the following tasks manually, even though you are using the IW:

- All hardware installation
- Tasks in Before Going to the Customer Site on page 130
- Any tasks related to adding LSPs to the primary controller you are installing, as documented in Administer Communication Manager on page 160:
- Any tasks related to administration of the primary controller in Administer Communication Manager on page 160
- Set Up SNMP Alarming on the G700 on page 511, if required

Electronic Worksheets and Templates

The IW can be used either with or without the Electronic Pre-installation Worksheet (EPW). It is recommended that you use the EPW with the IW.

To enable the IW to automatically configure and install the system, obtain the following Excel spreadsheet files from the project manager and load them onto your laptop:

- Electronic Pre-installation Worksheet
- Names/Number List Template (for S8300/G700 only)
- Customization Template

Note:

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

Electronic Pre-installation Worksheet

For greatest efficiency, obtain the Electronic Pre-Installation Worksheet (EPW), which is filled in by the customer and Avaya project manager. This worksheet is an Excel spreadsheet from which IW automatically pulls data to configure and install the S8300/S8500/S8700/S8710 Media Servers, G350/G700 Media Gateways, P330 Stack Processor, and VoiP Engines.

The EPW also can be used to supply basic translations for the S8300/G700 configuration.The default values used by the wizard can be viewed at http://support.avaya.com/avayaiw under the "View Default Parameters" link. If the wizard defaults do not meet the customer's needs, you can use a custom template.

Once the EPW has been imported, all the values from the EPW appear as defaults in the wizard.

Names/Number List Template (for S8300/G700 only)

The Names/Number Template, like the EPW, is an Excel spreadsheet that contains user administration data. The IW pulls this data to automatically administer users on the new system. This administration includes users' names, extensions, telephone types, classes of service, languages, locations, and voice mail capability. The native display name (unicode) is included.

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.

Customization Template

The Customization Template is a third Excel spreadsheet that allows automatic administration of key custom Communication Manager translations.

These translations are:

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

About the Upgrade Tool

The Upgrade Tool allows you to schedule automatic upgrades of Local Survivable Processors (LSPs) and G350 and G700 Media Gateways from the primary controller. The primary controller can be an S8300, S8500 or an S8700/S8710. With the upgrade tool, you do not have to physically be at the LSP and gateway locations in order to perform the upgrades. Additionally, you do not have to run the upgrades one by one. You simply enter the needed information for all LSPs, G350s, and G700s into the upgrade tool. Then, at the scheduled time, the Upgrade Tool automatically upgrades the software and firmware on all the specified LSPs and gateways.

Note:

You must still complete the normal prerequisite tasks such as completing the RFA process for license files and downloading the most recent .tar file (for an LSP) to the /var/home/ftp/pub directory or uploading the most recent firmware (for a media gateway) to a TFTP server.

The Upgrade Tool ships with the media servers and is available on the home page of the media server's Maintenance Web Interface. For more information, see *Job Aid: Upgrade Tool and Worksheets, 555-245-757*.

You cannot use the Upgrade Tool to:

- Install a new LSP or G350 or G700 Media Gateway.

  For each new installation, you must be on site and use the Avaya Installation Wizard (for an LSP), the Avaya Gateway Installation Wizard (for a media gateway), or perform a manual installation.

- Upgrade LSPs that require remastering the hard drive.

  This includes upgrading Communication Manager from 1.x to 2.x and migrating an S8300 version A to version B (the B version is required for release 2.1 and later).

- Upgrade an active LSP (which has taken control of calls because of a problem with the primary controller).
- Upgrade the S8300 Media Server acting as the primary controller.
- Upgrade an S8500 or S8700/S8710 Media Server.
- Upgrade X330 Expansion modules.
- Upgrade G600, G650, CMC1, SCC1, or MCC1 Media Gateways.

About the Avaya Gateway Installation Wizard

Use the Avaya Gateway Installation Wizard (GIW) to configure a new G350 or G700 Media Gateway that is controlled by a remote media server but does not have an S8300 installed in slot V1. The GIW enables you to configure the gateway IP addresses without having to enter CLI commands. You can also use the GIW to install firmware on the G700 and its components.

Use the GIW to configure a new G700 Media Gateway that is controlled by a remote S8300, S8500, or S8700/S8710 Media Server and that does *not* have an S8300 LSP.

Note:

To use the GIW to install firmware on the G700, you must first complete the normal pre-installation tasks such as downloading the most recent firmware to a TFTP server. Also, you cannot use the GIW to configure an X330 Expansion module.

The GIW can be accessed online at http://support.avaya.com/avayaiw. For more information, see *Job Aid: Avaya Gateway Installation Wizard,* 555-245-756.

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

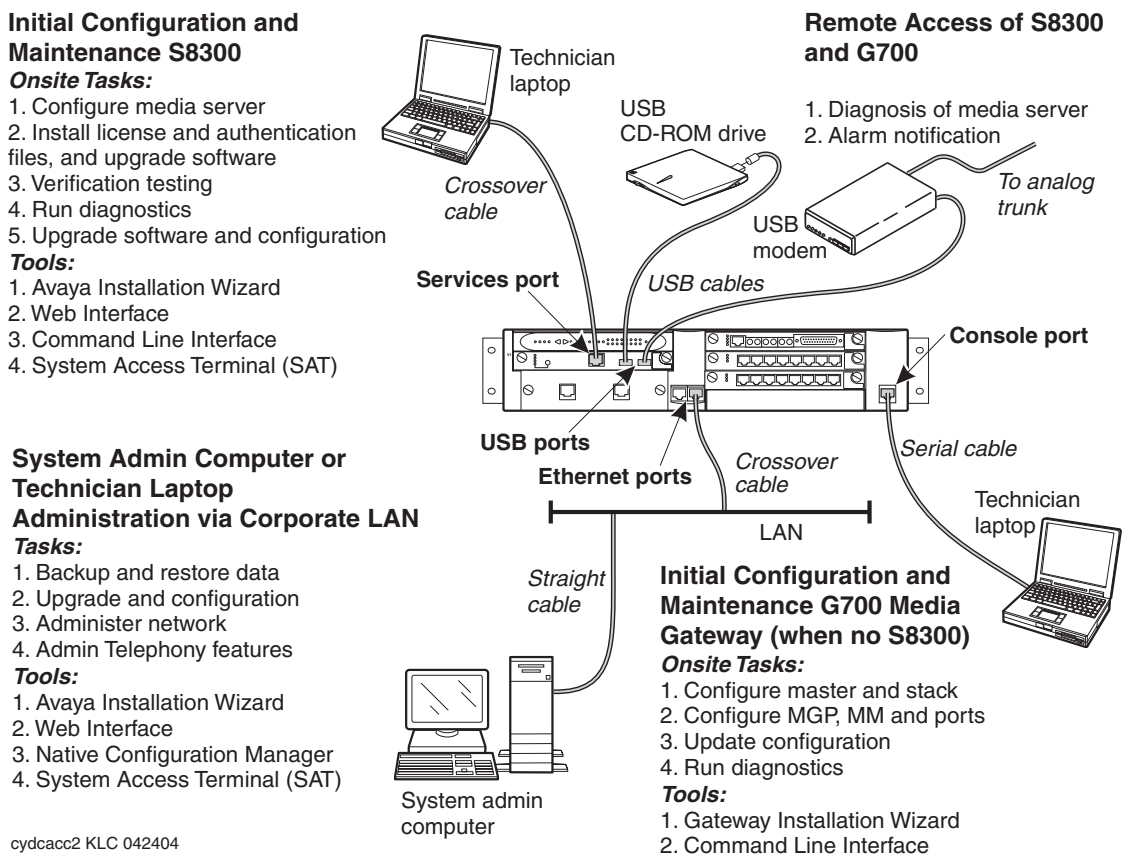
What physical access methods are available

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, S8500, or S8700/ S8710 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: 1**92.11.13.5**
   - 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 3 for pinout connections if needed. Crossover of the transmit and receive pairs (as shown) is required.

Table 3: 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 a Telnet 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 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 62), 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 a telnet session to the S8300:

    Type **`telnet <ip-address>`**, where ***`<ip-address>`*** is the **Server** 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**.
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 66.

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 59.
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 **9500** 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 66.

About Log in Methods

This section describes how to log on to the S8300, S8500, or S8700/S8710 media servers using 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, S8500, or S8700/S8710 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.

Logging in to the media server from your laptop using Telnet

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**.

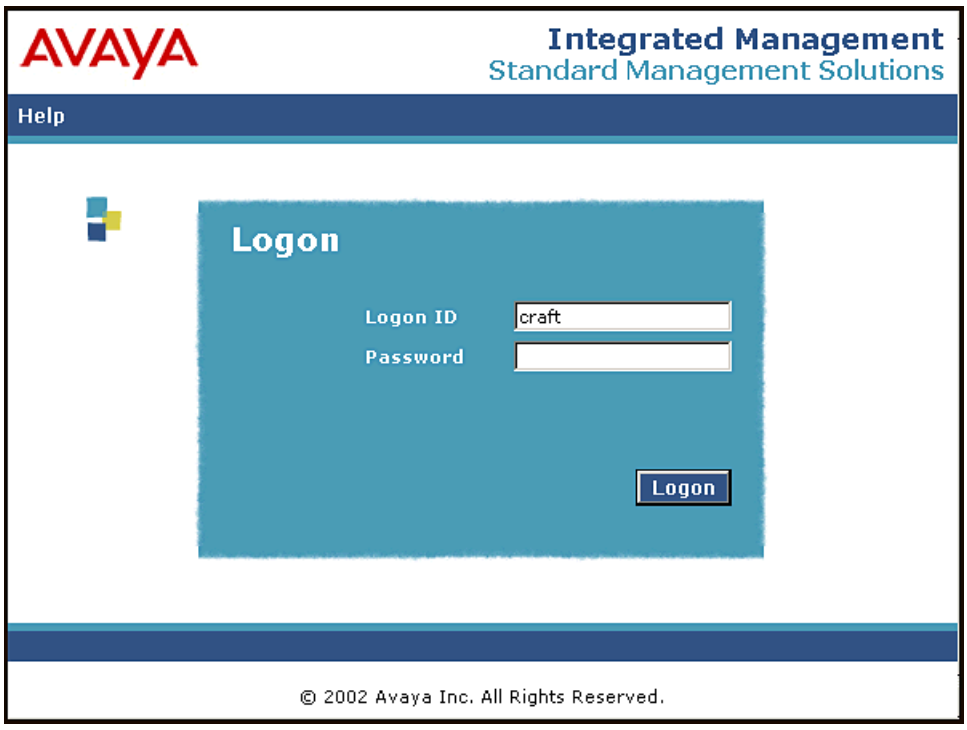
   If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate.
3. The system displays the **Welcome** screen.

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.

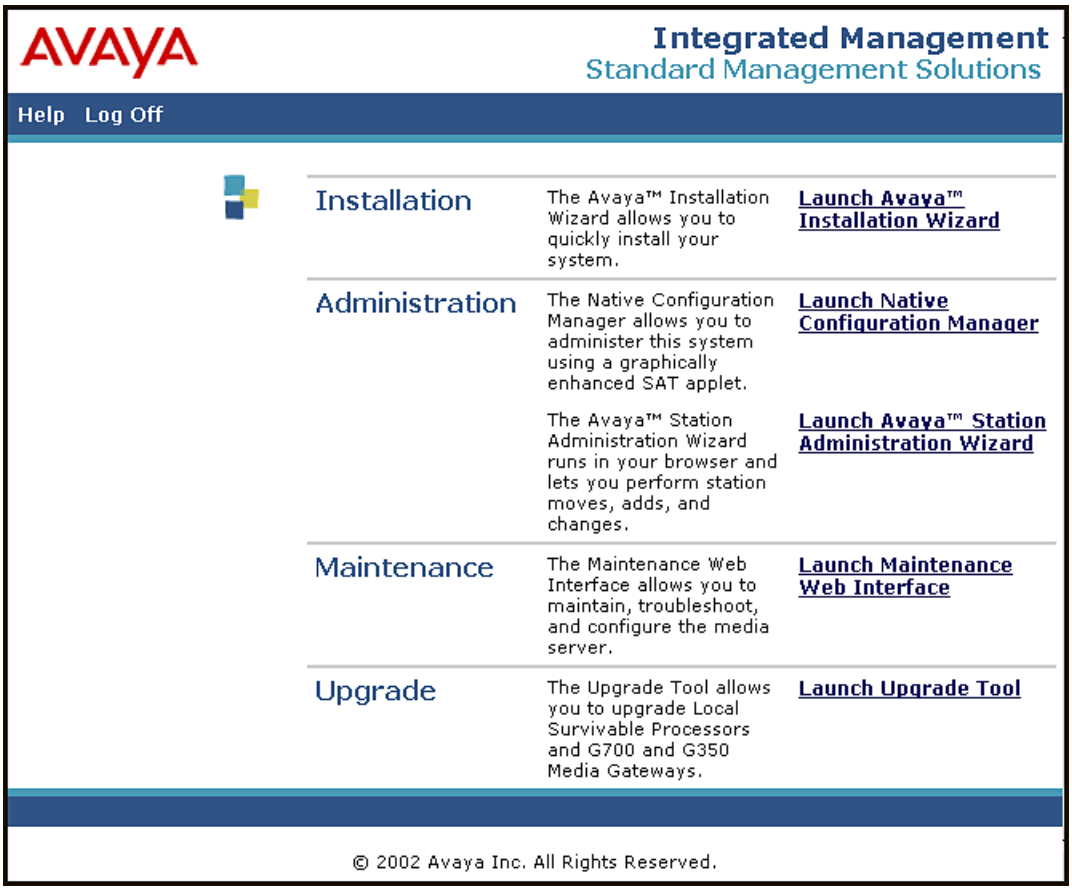
Login Screen



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



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

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 telnet session in progress, access the SAT program by typing **sat** or **dsat** at the telnet prompt.

   Or, to open SAT directly from your laptop:

   a. Click **Start > Run**

   b. Type **telnet 192.11.13.6 5023,** and press **Enter**.

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, telnet to the S8300 IP address.

   Type `telnet 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 69.

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 4 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 4: 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.

Differences between CLI commands for the G700 and G350 are described in an Application Note available at the Avaya Resource Library.

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 5 as a guide for **ntt** terminal emulation.

Table 5: 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 6 lists key presses for **w2ktt** terminal emulation.

Table 6: 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, S8500, or S8700/S8710 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: Avaya G700 Media Gateway Hardware Installation*, 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

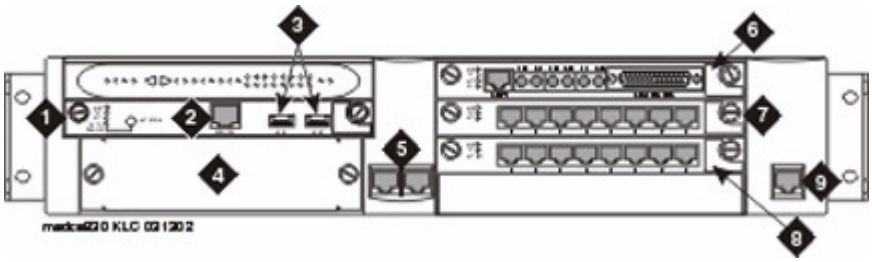


Figure notes:

1. **Media module slot #1 (V1)**
2. **S8300 services port (used with cross-over ethernet cable)**
3. **S8300 USB ports**
4. **Expansion module slot**
5. **10/100 Base-T Ethernet ports (ext1, ext2)**
6. **Media module slot #2 (V2)**
7. **Media module slot #3 (V3)**
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 77):

Figure 3: Media modules

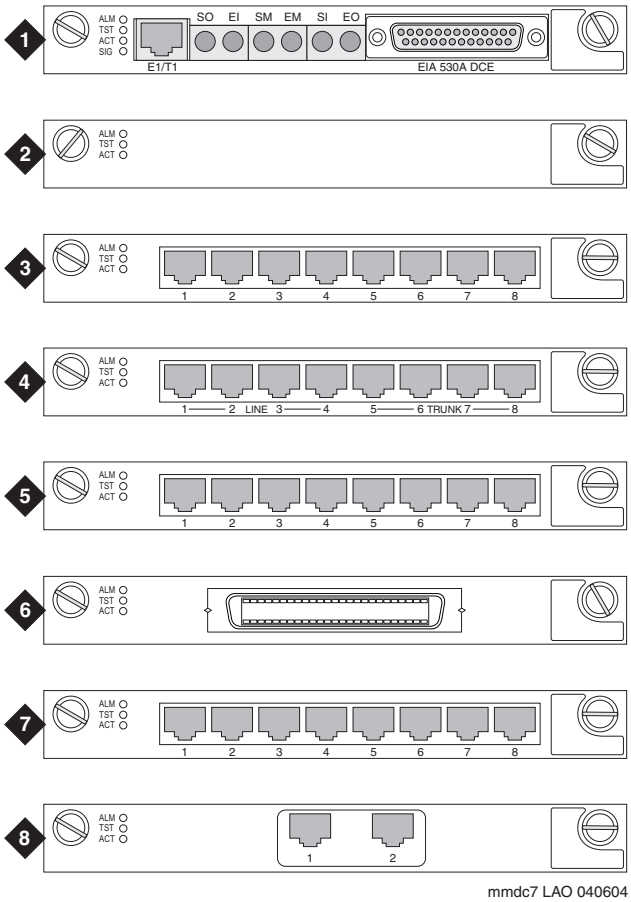


Figure notes:

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 MM717 DCP Media Module for connection to 24 DCP stations (*see the Caution below* for limitations on the use of the MM717)**
7. **Avaya MM720 BRI Media Module for connection to 8 ports for international BRI trunks or BRI endpoint (telephone and data module) connections**
8. **Avaya MM722 BRI Media Module for connection to 2 ports for international BRI trunks**

For detailed descriptions of the media modules see *Hardware Guide 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:

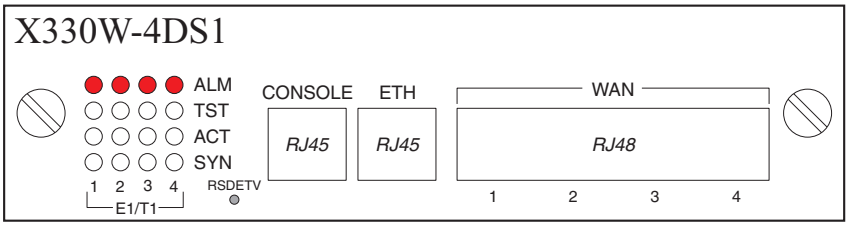
A shielded cable for the MM710 Media Module is required to meet emission requirements in European Union countries. The use of a shielded cable for the MM710 is preferred for installations worldwide.

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 MultiService Network Manager
- 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
- Simple API for XML (SAX) capability

The available C360 switch models are as follows:

- C363T Multilayer switch

  This switch has 24 10/100 Mbps ports and two 1-Gigabit Ethernet ports. Maximum power consumption is 45 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 45 Watts. Its power output per PoE port is 12.5 Watts.

- C364T

  This switch has 48 10/100 Mbps ports and two 1-Gigabit Ethernet ports. Maximum power consumption is 55 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 55 Watts. Its power output per PoE port is 15 Watts.

A C360 switch can co-reside in a stack with G700 Media Gateways. As a result, a C360 switch can be used as an expansion module for a G700 Media Gateway. 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.

  The Avaya C360 BUPS can support up to four Avaya C360 switches.
- 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

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.
- The green TST 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.

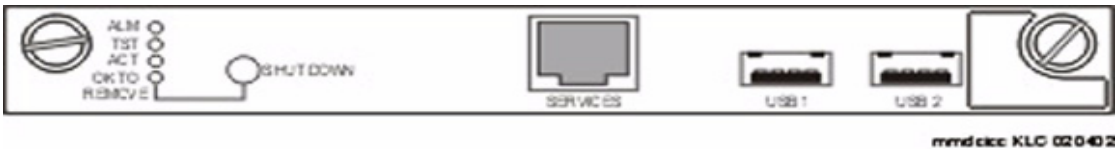
When you first power up the S8300, the red Major Alarm LED lights. During startup, an LED sequence runs: red ALM, green TST, yellow ACT, green OK-to-Remove, and the three LEDs under the Services Port, after which all LEDs turn off. At this point, you can connect to the S8300. When Communication Manager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



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 S8300B Media Server has:

- Avaya Communication Manager (For a full description see: http://www.avaya.com/support)
- Administration and maintenance provisioning software
- 20 G or 30 G hard drive
- 512 MB RAM (in two 256 MB DIMM strips)
- Web server
- Linux OS (Red Hat)
- Support of H.248 and H.323 Protocols
- TFTP server and other IP services

Note:

The current version (B) of the S8300 is 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 Guide for Avaya Communication Manager,* 555-245-207).

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.

What is the S8700/S8710 media server

The G700 Media Gateway can be controlled by an external S8700/S8710 Media Server (sometimes referred to as an ECC configuration). Both the S8700/S8710 with the G600 Media Gateway (IP Connect) and the 8700 with the SCC1 or the MCC1 Media Gateways (Multi-Connect) can control the G700. The S8700/S8710 is connected to the G700 over the network through a C-LAN circuit pack in the G600, SCC1, or MCC1.

Information on installing the G700 using the S8500 or S8700/S8710 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
- Uninteruptible Power Supply (UPS)
- Universal Serial Bus (USB) Modems

See Chapter 8: 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.

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.

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, 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 86
- Verifying Environmental conditions on page 87
- Unpacking and checking the order on page 88
- Installing the G700 media gateway on page 88
- Cabling multiple units on page 99
- Attaching Ground Conductors on page 103

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

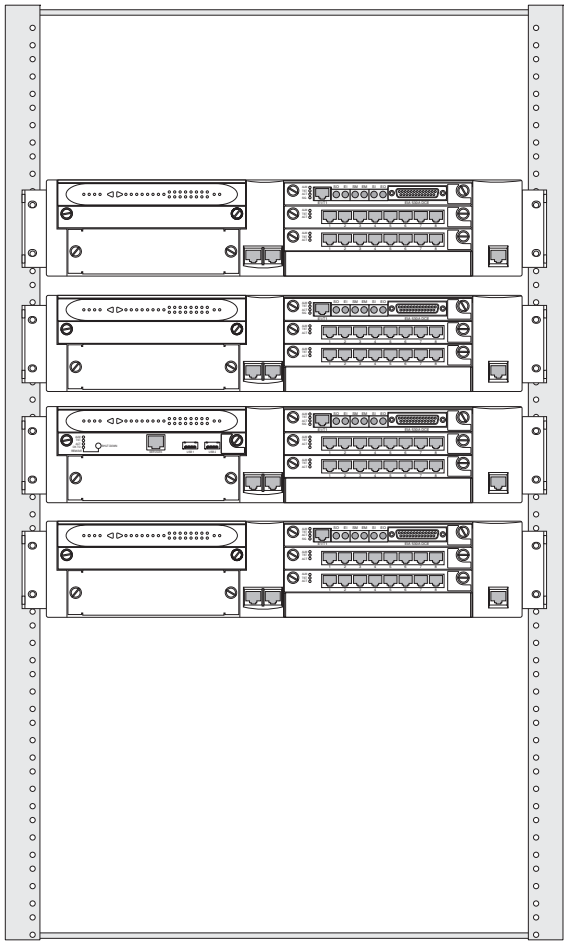
After you have verified the site conditions and the shipment, you proceed with the installation of the hardware.

Perform the following steps:

- Preparing the G700 media gateway on page 89
- Mounting the G700 media gateway in the rack on page 90

Figure 6: Avaya G700 Media Gateways on page 89 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



scdcrck4 LAO 030203

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

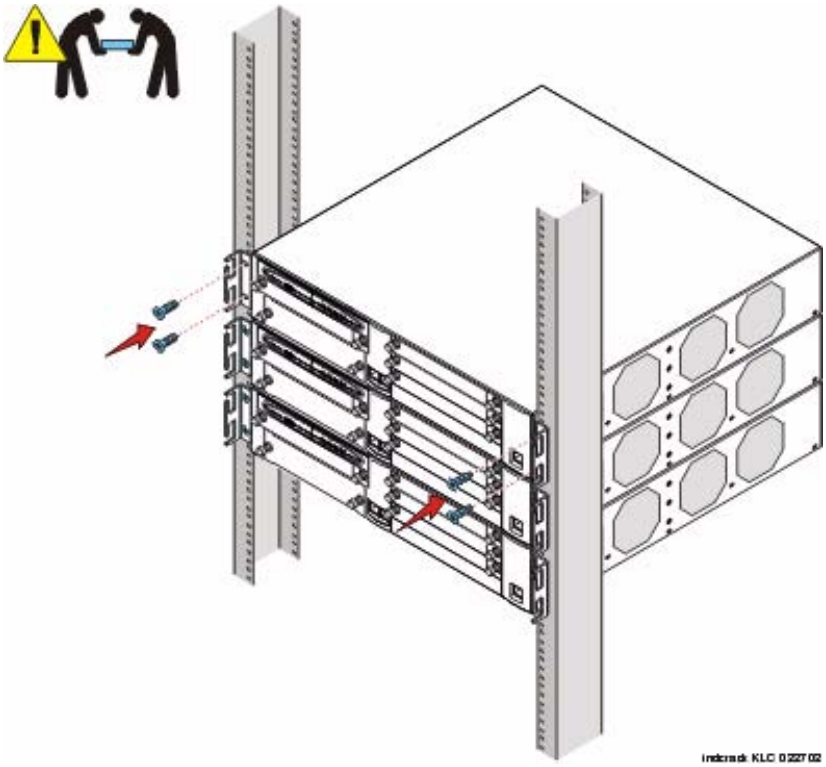
The G700 Media Gateway mounts in a standard 19-inch rack. It is held in place by screws through the two mounting ears. The unit can be mounted either in the center of the unit or at the front of the unit; however, only the front mount allows use of the guides for electrical cables. To avoid balancing 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 100); 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. The LED module must be pulled from the G700 chassis to provide clearance for the S8300 Media Server.

Tip:

If you need to install the CWY1 card (for embedded messaging) on the S8300, do so now. Starting with Communication Manager Release 2.2, the CWY1 card is no longer needed.

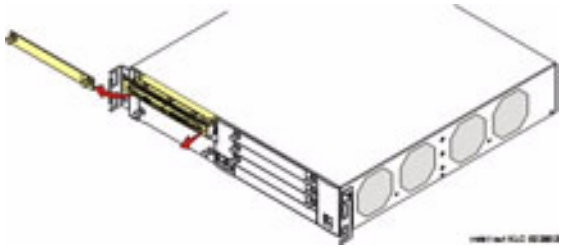
CAUTION:

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.

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

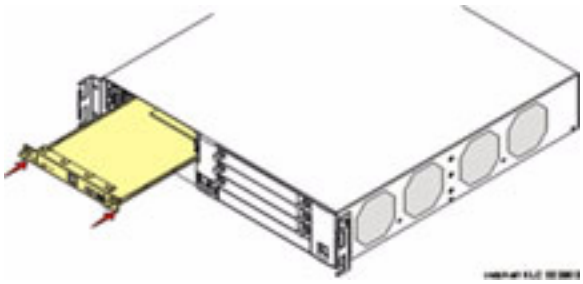
1. Clear the left side of the G700 Media Gateway.
   a. Remove the blank plate from slot #1.
   b. Then, disengage the LED module and remove it from the G700 Media Gateway.
2. Line up the Avaya S8300 Media Server module squarely with its bay opening.

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.

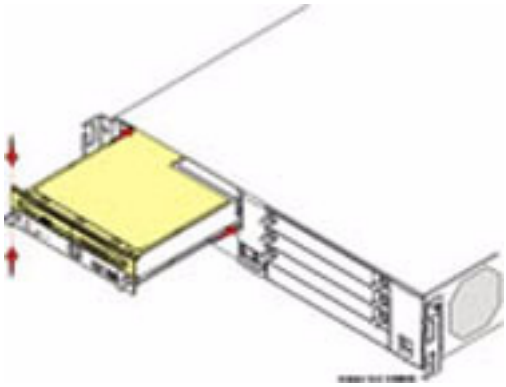
Figure 9: Insert S8300



4. 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. 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.
6. Apply firm pressure to engage the connectors.

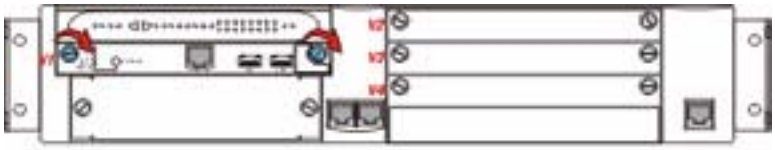
   The connector has different length pins. The long pins will engage first to provide grounding. Medium length and short pins will provide power and signal.

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



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
- 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 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 Guide 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 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.

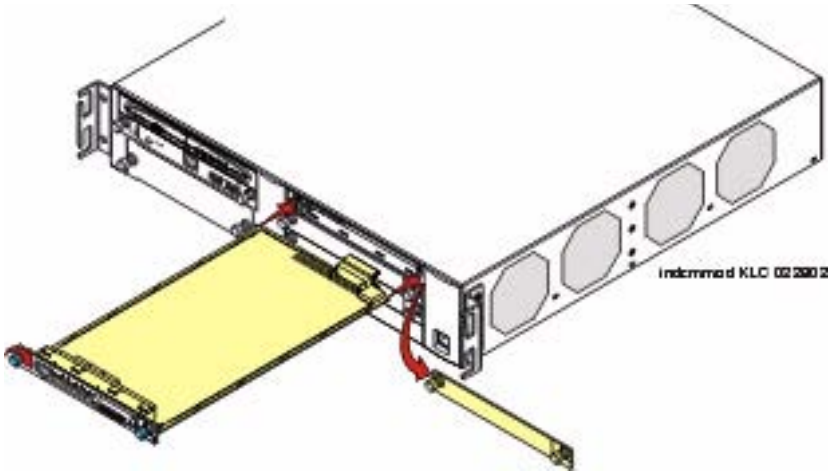
CAUTION:

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 360).

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 76).

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.

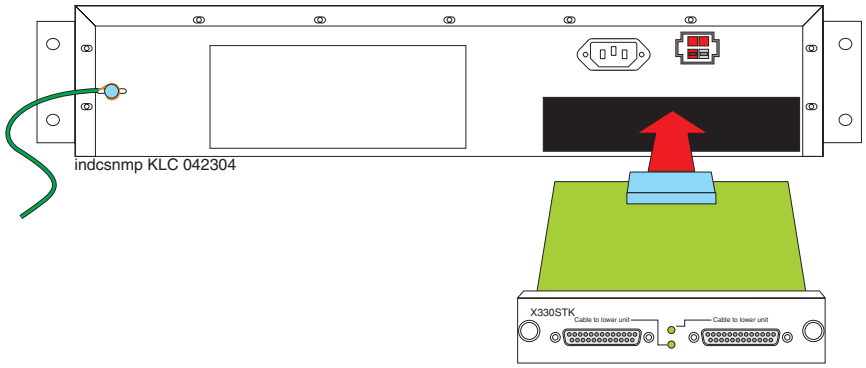
CAUTION:

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

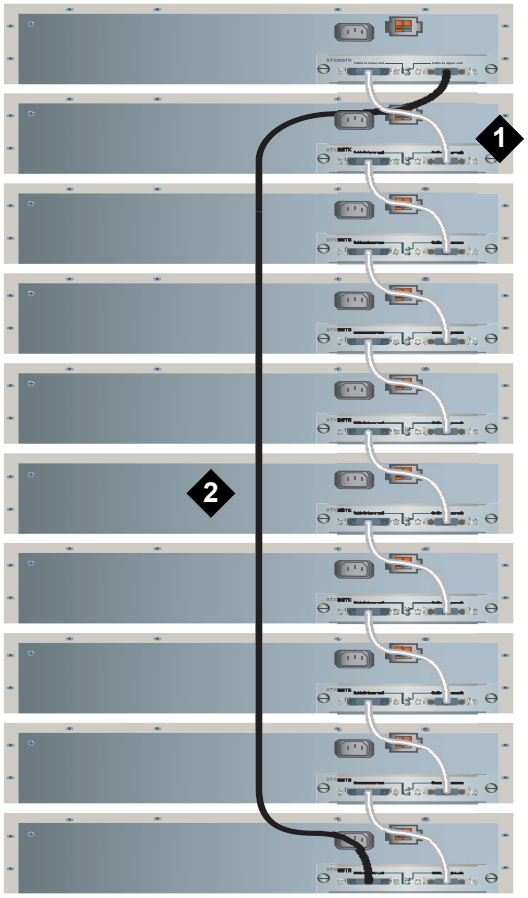


Figure notes:

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

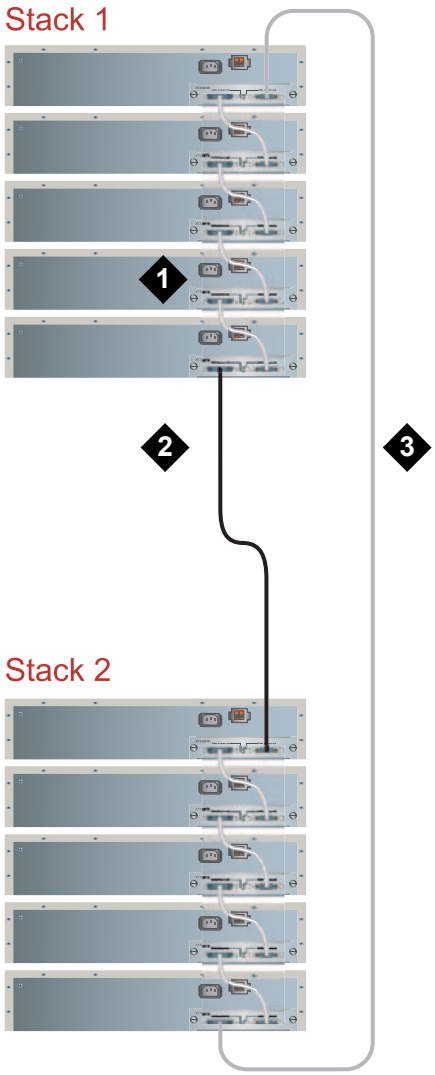


Figure notes:

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 mm^2) 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 (26mm^2) 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 mm^2), 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 $mm^{2)}$ 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 ($4mm^2$) 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:

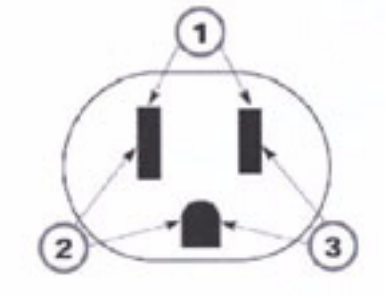


Figure notes:

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
   b. TST - 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 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.

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).

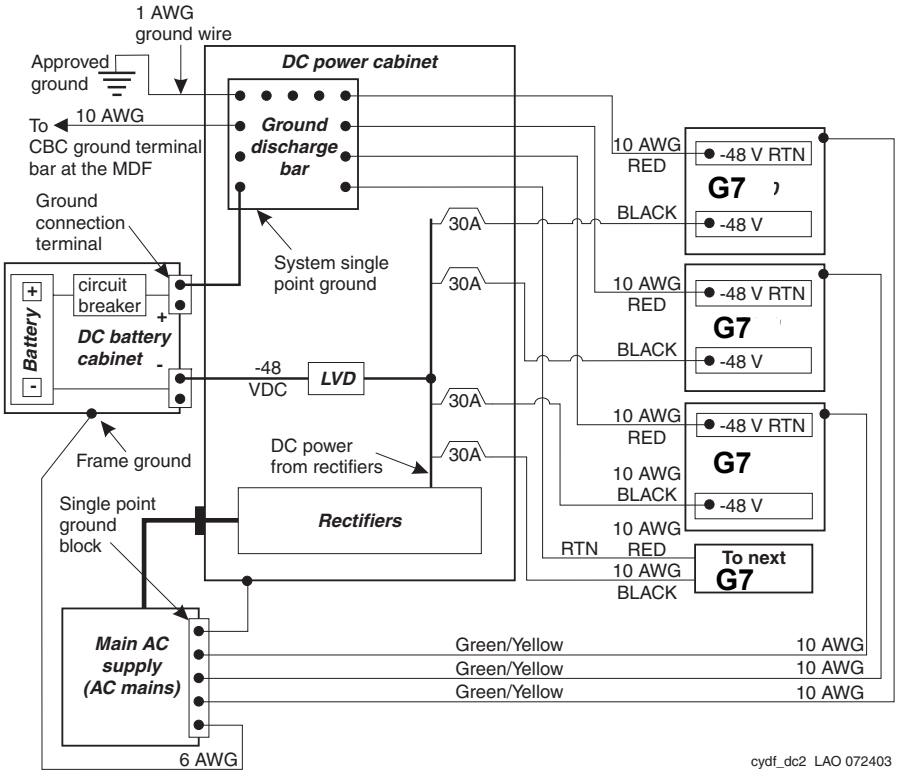
To check DC power

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, 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 8: 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
- Chapter 4: Installing a new G700 without an S8300
- Chapter 5: Upgrading an existing S8300A to R3.0 using the Wizards
- Chapter 6: Upgrading an existing S8300B to R3.0 using the Wizards
- Chapter 7: Upgrading an existing G700 without an S8300

  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	G700 Controlled by an S8300 with IA 770 INTUITY AUDIX Messaging
New Installation	Checklist 1 Chapter 2 Chapter 3	Checklist 2 Chapter 2 Chapter 4	See *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532
Upgrade an Existing System	S8300A to R3.0: Checklist 3 Chapter 5 S8300B to R3.0: Checklist 4 Chapter 6	Checklist 5 Chapter 7	

Checklist 1: Install a New G700 with an S8300 (Primary or LSP)

Use Checklist 1 to install a G700 Media Gateway with the following characteristics:

- The G700 has an S8300 Media Server configured as the primary controller

  or,

- The G700 has an S8300 Media Server configured as an LSP and is controlled by an S8300, S8500, or an S8700-series Media Server.

You will use Chapters 2 and 3 with this checklist.

For help with connecting to and logging in to the G700 or S8300, see About connection methods on page 54.

Checklist 1: Install New G700 with an S8300 (Primary or LSP)

Major Tasks	Subtasks
Installation Overview on page 126	- G700 components - Software and firmware files - Access to the Server CD - Access to the S8300 and G700
Before Going to the Customer Site on page 130	- Install TFTP Server or Obtain USB CD Drive - Get planning forms - Get the G700 serial number - Check FTP server for backups - Obtain service pack files, if needed - If using IA770, obtain service pack and language files, if needed - If using IA770, obtain Ethernet interface IP address and Subnet mask - Complete the RFA process - Obtain static craft password
Hardware installation for the G700 Media Gateway and S8300 Media Server on page 75	- On site checklist - Unpack and check the order - Install the G700 - Cable multiple units - Attach ground conductors
Install the S8300 on page 137	- Insert the S8300 - Remaster the hard drive and install new CM software, and IA770 software, if necessary -Using the Avaya Installation Wizard (IW) on page 148: --Set time, date, and time zone --Import EPW --Set usage option
Configure the S8300 (See Using the Avaya Installation Wizard (IW) on page 148	- Set server identities - Configure Stack Master/IP routes - Configure optional services: UPS DNS NTP INADS - Load Security files - Install CM software --Upload translations, if necessary

Checklist 1: Install New G700 with an S8300 (Primary or LSP) (continued)

Major Tasks	Subtasks
Configure the G700 Media Gateway (See Using the Avaya Installation Wizard (IW) on page 148	-Assign IP addresses to the G700 processors -Set up default IP route for the G700 -Check IP connections -Set up controller list for the G700 - Configure X330 Expansion Module, if necessary
Install new firmware on the G700 and media modules (See Using the Avaya Installation Wizard (IW) on page 148	-Verify contents of the tftp directory -Determine which firmware to install -Install firmware on the P330 Stack Processor -Install firmware on the G700 media gateway processor -Install firmware on the media modules -Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree
Installing IA770 service pack files, if any on page 157	- Log in to the S8300 platform - Install IA770 service pack, if any - Stop the system - Restart the system - Enable messaging on the S8300 Web interface, if necessary
Administer Communication Manager on page 160	- Reboot the system - Assign node names, if necessary - Administer network regions - Assign LSPs to network regions - Administer IP interfaces - Administer the LSP form - Add media gateway - Verify changes - Enable announcements, if necessary - Save translations
Considerations for IP Phones Supported by a Local Survivable Processor on page 177	
Complete the Installation of the S8300 (if the Primary Controller) on page 179	- Register the system - Back up the system - Check planning documentation - Connect and administer test endpoints - Complete electrical installation - Enable adjunct systems

2 of 3

Checklist 1: Install New G700 with an S8300 (Primary or LSP) (continued)

Major Tasks	Subtasks
If using IA770, administer Communication Manager for Integrated Messaging on page 180	
Complete the Installation Process (for an S8300 LSP) on page 181	- Check planning documentation - Connect and administer test endpoints - Complete electrical installation - Enable adjunct systems

3 of 3

Checklist 2: Install a New G700 without an S8300

Use Checklist 2 to install a G700 Media Gateway with the following characteristics:

- The G700 does not have an S8300 and is controlled by an external S8300, S8500, or S8700-series Media Server.

You will use Chapters 2 and 4 with this checklist.

For help with connecting to and logging in to the G700, see About connection methods on page 54.

Checklist 2: Install a New G700 without an S8300

Major Task	Subtasks
Before going to the customer site on page 187	- Get planning forms - Get the G700 serial number - Install the Gateway Installation Wizard - Set up TFTP server, if necessary - Download firmware files
Hardware installation for the G700 Media Gateway and S8300 Media Server on page 75	- On site checklist - Unpack and check the order - Install the G700 - Cable multiple units - Attach ground conductors

1 of 2

Checklist 2: Install a New G700 without an S8300 (continued)

Major Task	Subtasks
Collecting Installation Information on page 187	- Obtaining planning forms - Getting the Serial Number of the G700, if Necessary - Installing the Gateway Installation Wizard - Setting Up the TFTP Server - Downloading G700 firmware files to your TFTP directory
Configure the G700 on page 190	- Assign IP addresses to the G700 processors - Set up IP routing for the stack - Set up default IP route for the G700 - Check IP connections - Set up controller list for the G700 - Configure X330 Expansion Module, if necessary
Install firmware on the G700 and media modules on page 191	- Install firmware on the P330 Stack Processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree
Administer Communication Manager on page 193	- Reboot the system - Assign node names, if necessary - Administer network regions - Assign LSPs to network regions - Administer IP interfaces - Administer the LSP form - Add media gateway - Verify changes - Enable announcements, if necessary - Save translations
Complete the Installation Process on page 209	- Check planning documentation - Connect and administer test endpoints - Complete electrical installation - Enable adjunct systems

2 of 2

Checklist 3 Upgrade an Existing G700 with an S8300A to R3.0

Important:
You must replace the S8300A with an S8300B for this upgrade.

Use Checklist 3 to upgrade a G700 Media Gateway with the following characteristics:

- The G700 has an S8300A Media Server configured as the primary controller.

  or,

- The G700 has an S8300A Media Server configured as an LSP and is controlled by either an S8300, S8500, or S8700-series Media Server.

You will use Chapter 5 with this checklist. For help with connecting to and logging in to the G700 or S8300, see About connection methods on page 54.

Checklist 3: Task List to Upgrade an Existing G700 with an S8300A (R1.x or R2.0.x to R3.0)

Major Tasks	Subtasks
Before going to the customer site on page 214	- Install TFTP server or obtain USB CD drive - Fill in EPW (if upgrading from 1.1) - Get planning form - Get the G700 serial number - Check number of allocated ports - Check FTP server for back up - Get software/firmware files - Download Communication Manager service pack and IA770 service pack software to laptop, if necessary - Complete the RFA process - Obtain static craft password
Preparing for the upgrade on-site on page 224	- Check current software release - Pre-Upgrade tasks — If the Target S8300 is the Primary Controller - Get IA770 data and stop IA770 - Back up system files - Record configuration information

1 of 2

Checklist 3: Task List to Upgrade an Existing G700 with an S8300A (R1.x or R2.0.x to R3.0) (continued)

Major Tasks	Subtasks
Upgrading the S8300A on page 237	- Install the pre-upgrade service pack - Linux Migration Backup - Replace the S8300A - Remaster and Upgrade the S8300: - Verify software version - Copy licence and authentication files to the S8300 - Disable messaging - Configure S8300 network parameters - Verify connectivity to backup server - Restore backup data - Verify date and time - Install post-upgrade service pack, if necessary - Verify S8300 configuration - Install license file, if necessary - Install authentication file, if necessary - Save translations (if not using IA770) - Verify operation
Upgrade the firmware on the G700 Media Gateway on page 268	- Decide whether to use the Installation Wizard If not using the Wizard: - Verify contents of the tftp directory - Determine which firmware to install - Install firmware on the P330 Stack Processor -Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any - Set Rapid Spanning Tree If using IA770: - Install and restart IA770 - Save translations - Install IA770 service pack, if any - Install optional language files, if any
Complete the upgrade process (S8300 is the primary controller) on page 277	- Check media modules - Enable scheduled maintenance - Busyout trunks - Check for translation corruption - Resolve alarms - Re-enable alarm origination - Back up system - Restart LSPs, if any

2 of 2

Checklist 4 Upgrade an Existing G700 with an S8300B to R3.0

Use Checklist 4 to upgrade a G700 Media Gateway with the following characteristics:

- The G700 has an S8300B Media Server configured as the primary controller.

  or,

- The G700 has an S8300B Media Server configured as an LSP and is controlled by either an S8300, S8500, or S8700-series Media Server.

You will use Chapter 6 with this checklist. For help with connecting to and logging in to the G700 or S8300, see About connection methods on page 54.

Checklist 4: Task List to Upgrade an Existing G700 with an S8300B (R2.0.x to R3.0)

Major Tasks	Subtasks
Before going to the customer site on page 280	- Get planning form - Get the G700 serial number - Check number of allocated ports - Check FTP server for back up - Get software/firmware files - If using IA770, obtain service pack and language files, if any - Complete the RFA process - Obtain static craft password - Download service pack software to laptop, if necessary
On-site Preparation for the Upgrade on page 288	- Pre-Upgrade tasks — If the Target S8300 is the Primary Controller - Get IA770 data and stop IA770 - Back up recover system files - Install new license and authentication files, if necessary - Save translations, if new license and/or authentication files installed - Transfer files from CD or laptop
Upgrade the S8300 on page 307	Install the Upgrade Software: - Install Communication Manager pre-upgrade service pack - Upgrade S8300, using Web Interface Manage Software screens - Make the upgrade permanent

1 of 2

Checklist 4: Task List to Upgrade an Existing G700 with an S8300B (R2.0.x to R3.0) (continued)

Major Tasks	Subtasks
Upgrade the G700 Firmware on page 314	- Use the Avaya Installation Wizard or the Upgrade Tool - Verify contents of the tftp directory - Determine which firmware to install - Install firmware on the P330 Stack Processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree
Installing IA770 service pack (or RFU) files, if any on page 319	
Completing the upgrade process (S8300 is the primary controller) on page 320	- Check media modules - Enable scheduled maintenance - Busy out trunks - Check for translation corruption - Resolve alarms - Re-enable alarm origination - Back up system - Restart LSPs, if any

2 of 2

Checklist 5: Upgrade an Existing G700 without an S8300

Use Checklist 5 to upgrade a G700 Media Gateway with the following characteristics:

- The G700 does not have an S8300 and is controlled by an external S8300, S8500, or S8700-series Media Server.

You will use Chapter 7 with this checklist. For help with connecting to and logging in to the G700, see About connection methods on page 54.

Checklist 5: Task List to Upgrade an Existing G700 without an S8300

Major Tasks	Subtasks
Before going to the customer site on page 325	- Get planning forms - Get the G700 serial number - Set up TFTP server, if necessary - Install the Gateway Installation Wizard on laptop - Download firmware files
On-site preparation for the upgrade on page 328	- Verify contents of the tftp directory - Determine which firmware to install
Installing new firmware on the G700 Media Gateway on page 331	Using the Upgrade Tool: - Install firmware on the P330 Stack Processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree

Chapter 3: Installing a new G700 with an S8300

This chapter covers the procedures to install a new Avaya G700 Media Gateway with an Avaya S8300B 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*** Communication Manager software installed on the hard drive. The hard drive contains only the remastering program (RP) software, which remasters the hard drive and installs the Communication Manager Software from the Server CD. To install the software, you need to have the Avaya TFTP Server installed on your laptop or use an external USB CD-ROM drive.

However, the S8300B may occasionally ship with Communication Manager software installed. In this case you must use an external USB CD-ROM drive — you cannot use the TFTP server on the laptop. See About access to the Server CD on page 127 for more information.

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.

Important:

This installation procedure requires that TFTP server software is installed on the technician's laptop. If the TFTP server is not installed on the laptop, you can use an external USB CD-ROM drive instead.

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

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 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 148) and install G700 firmware (Install new firmware on the G700 on page 146) 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 G700 components

A P330 Stack Processor is built into the G700 Media Gateway. (This processor is also known as the *Layer 2 switching processor*). The G700 also contains an MGP processor, a VoIP processor, and media modules. Updating the firmware for one or more of these processors and/or media modules is a required part of most S8300 software upgrades.

About software and firmware files

A new S8300 Media Server should have only the remaster program (RP) software installed on its 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.

The file containing the S8300 software and G700 firmware has a *.tar extension. The *.tar file is on the “Unity” 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 Server CD

The R3.0Communication Manager software and other files needed for the R3.0upgrade are on the Server CD that you take to the customer site.

You can make the Server CD available to the upgrade process in one of two ways:

- ***Recommended:*** Place the CD in the CD-ROM drive on the technician's laptop. This method requires that the Avaya TFTP Server software (available at support.avaya.com) is installed on the technician's laptop. This method requires that the S8300B ***does not*** have Communication Manager software installed on its hard drive.

  or,

- Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate. This method works whether or not Communication Manager software is installed on the S8300B hard drive.

  Important:

  Before you go the site, you must either have the TFTP server installed on your laptop (recommended) or have an external USB CD-ROM drive.

  The new S8300B will normally not have Communication Manager software installed on its hard drive. You should check the S8300B that you will be installing (or ask the customer to check) before going to the site to determine whether you need to have the external USB CD-ROM drive. If software is not installed, the label on the hard drive will say "S8300B Hard Drive Without CM Software." If software is installed, the label will indicate the software release. If software is installed, you must use the external USB CD-ROM drive because the TFTP server on your laptop will not work.

This chapter describes the upgrade procedure with the TFTP Server software installed on the laptop and using the laptop CD-ROM drive as source of the upgrade software. For instructions on obtaining and installing the Avaya TFTP Server, see Appendix D: Install the Avaya TFTP server

System Access

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.

How is normal access to the S8300 and G700 provided

You can access the S8300 and G700 in several ways with either a direct connection or LAN connection.

Note:

Before the Upgrade Tool can be used to upgrade software on an LSP or firmware on a G700, as summarized below, the LSP must be administered on the primary controller.

Connecting directly to a target S8300

If you are at the location of the target S8300 (primary or LSP), you can connect directly to the S8300 Services port.

To install or upgrade directly

1. Install the S8300 software by:
   - Opening the Web interface and using the Avaya Installation Wizard

     or,
   - Opening the Web interface and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or the Upgrade Tool

     or,
   - Opening a telnet session to the S8300, and then telnet to the P330 stack processor

Connecting directly to the remote primary server (S8300, S8500, or S8700)

In this case, the target S8300 is an LSP. If you are at the location of the remote primary server, you can connect directly to the remote server's Services port.

To install or upgrade the target LSP remotely

1. Install the S8300 (LSP) software by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool

     or,
   - Opening a telnet session to the primary server and then telnet to the P330 stack processor and perform the installation commands

Note:

For direct connections, the TFTP server must be on the Customer LAN, not on your laptop.

Connecting using the customer's LAN

If you can connect to the customer's LAN, you can:

1. Install the S8300 software by:
   - Opening the Web interface on the S8300 and using the Avaya Installation Wizard

     or,
   - Opening the Web interface on the S8300 and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface on the primary server and using the Avaya Installation Wizard or Upgrade Tool

     or,
   - Opening a telnet session to the P330 stack processor and perform the installation commands

Note:

For LAN connections, the TFTP server can be your laptop or a customer computer on the LAN.

See About connection and login methods on page 47 for details on how physically to connect and log into the G700.

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.

Perform the following pre-installation tasks:

Installing TFTP server (or obtaining USB CD-ROM drive)

Collecting Installation Information

Obtaining service pack files, if needed

If using IA770, obtaining service pack and language files

Completing the RFA process (Obtaining license and password file)

Installing TFTP server (or obtaining USB CD-ROM drive)

Installing Communication Manager on an S8300B requires remastering the S8300B hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on:

- Your laptop if a TFTP server is installed

  or,

- An external USB CD-ROM drive

You must have the Avaya TFTP server software installed on your laptop or take a USB CD-ROM drive to the site. If you do not already have the Avaya TFTP server installed on your laptop, you can obtain the software from the Avaya Support website and install it as described in Appendix D: Install the Avaya TFTP server.

Important:

If the new S8300B that you will be installing has Communication Manager software installed on its hard drive, you must use an external USB CD-ROM drive instead of the TFTP server on your laptop. See About access to the Server CD on page 127.

Collecting Installation Information

Planning forms provided by the Project Manager

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.

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 the FTP Server for Backing up Data

During the installation and upgrade procedures, you will need to back up the system data to an FTP server. Normally, you will use an FTP server on the customer's LAN for backups.

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

Check with your project manager or the customer for this information.

Important:
Before going to the customer site, make sure that you can use a customer server for backups.

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.

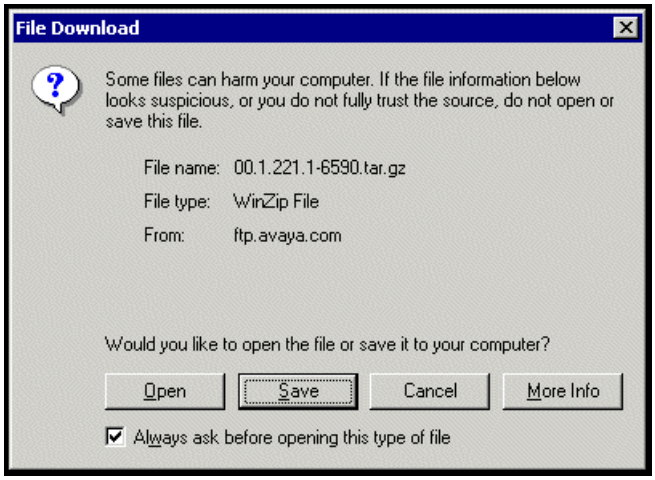
To download a pre-upgrade service pack

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 3.0**).
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.

If using IA770, obtaining service pack and language files

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 website, double click on **Find Documentation and Downloads by Product Name**.
2. Select:

   > **IA 770 INTUITY AUDIX Messaging Application**.

   > **Downloads**

   > **IA770 INTUITY AUDIX Embedded Messaging Application Patches**
3. Scroll down and double click on the desired service pack file name. For example, **C6072rf+b.rpm**.
4. 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 will download the appropriate language files from a language CD. The customer should have the language CDs at the site. If not, you need to obtain the appropriate language CDs and take them to the site.

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 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, S8500, S8700, S8710, or Blade 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.

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. When inserting the S8300 Media Server, the LED module (above slot V1) must also be removed or inserted together with the S8300.

   Disengage the LED module and the S8300 module and remove them together from the G700.

2. The LED panel (above slot V1) must be inserted together with the S8300 module.

   a. Insert both the LED panel and S8300 module 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).

   b. Push both modules (together) back into the guides, gently and firmly, until the front of each module aligns with the front of the G700.

3. Secure the S8300 faceplate with the thumb screws.

   Tighten the thumb screws with a screw driver.

4. Power up the G700 by plugging in the power cord.

5. Connect the laptop to the Services port on the faceplate of the S8300.

Installing Communication Manager Software

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 S8300B 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.
5. Insert the Server CD in the CD-ROM drive:
   - If TFTP server software is installed on your laptop, ***start the TFTP server program*** (TFTPServer32.exe), and insert the Communication Manager Server CD in the laptop's CD drive.

CAUTION:

Verify good AC power connections to the laptop. Do not attempt a remastering using only the laptop's battery power.

Note:

Shut down all applications on the laptop except for the TFTP server and the telnet client. Other background applications can overly use laptop resources.

Note:

Ensure that the **Outbound file** path is set to the root of your laptop's CD-ROM drive. (For example, D:\)

To check:

i. Open the **System** menu in the TFTP server program

ii. Select **Setup**

iii. Open the **Outbound** tab.

iv. To change the **Outbound file** path, click the **Browser** button and select the **CD** drive.

or,

- If your laptop does not have TFTP server software installed, attach an external USB CD-ROM drive to one of the USB ports on the S8300B and insert the Server CD in the drive.

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.

NOTE: If you get the login prompt instead of the RP screen

If the telnet login prompt appears instead of the RP screen, the hard drive contains a Communication Manager software release. In this case, if you have a USB CD-ROM drive, connect the drive to a USB port on the S8300 and insert the Server CD. Then log in to the telnet session (using the initial *craft* login) and use the **Shutdown Server** feature on the Maintenance Web Interface to reboot the system. After the reboot completes, telnet to 192.11.13.6 and the RP screen should now be displayed.

If you do not have the USB CD-ROM, you cannot proceed with the upgrade procedure described in this chapter. However, you can upgrade the Communication Manger software using the procedure described in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware and then return to this chapter.

To upgrade using the procedure in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware

1. Complete the procedures starting at Installing the pre-upgrade software service pack on page 658 and ending with Making the upgrade permanent on page 670. Note that you must have a copy of the license and authentication files on your laptop and install them before doing the upgrade.
2. Return to this chapter and complete the procedures starting with Using the Avaya Installation Wizard (IW) on page 148.
3. Complete all the remaining procedures, ***skipping*** installation of the license and authentication files, which was done in step 1.

Alternatively, you can obtain a USB CD-ROM drive or an S8300B with only the RP software and proceed from Remastering the hard drive and installing the software on page 138.

The first RP screen

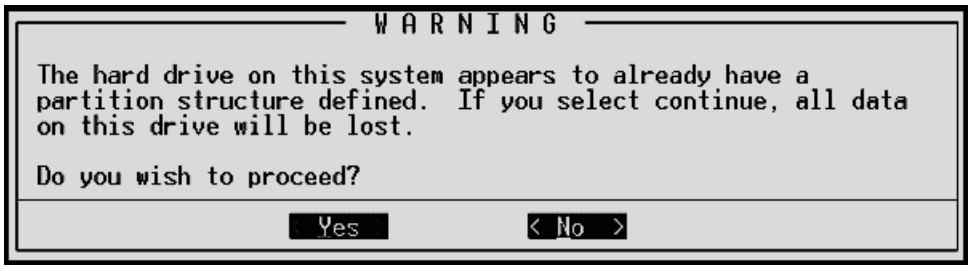
Tip:

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.

4. Select **Install** and press **Enter**.

   If a **Warning** screen appears,

RP Warning screen

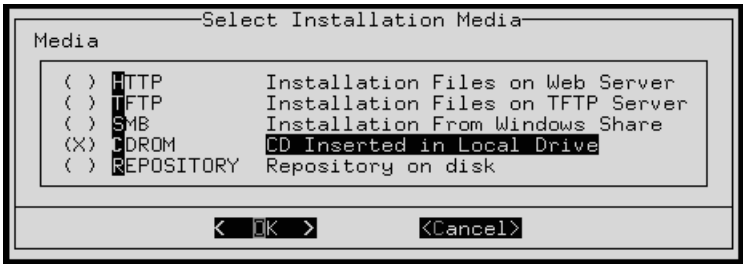


select **Yes** and press **Enter**.

Note:

At this point, the installation script looks for the Server CD either on your laptop or in a CD drive connected to the USB port. If you do not have the TFTP server running on the laptop, and a CD drive is not attached to a USB port, you will see the **Select Installation Media** screen:

The Select Installation Media screen



If you see the Select Installation Media screen:

a. Start up the TFTP server on your laptop, or connect a USB CD-ROM drive to one of the USB ports.

b. Insert the Server CD in the laptop or USB drive.

c. Select either **TFTP** or **CDROM**.

d. Select **OK,** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen

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

6. The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen

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

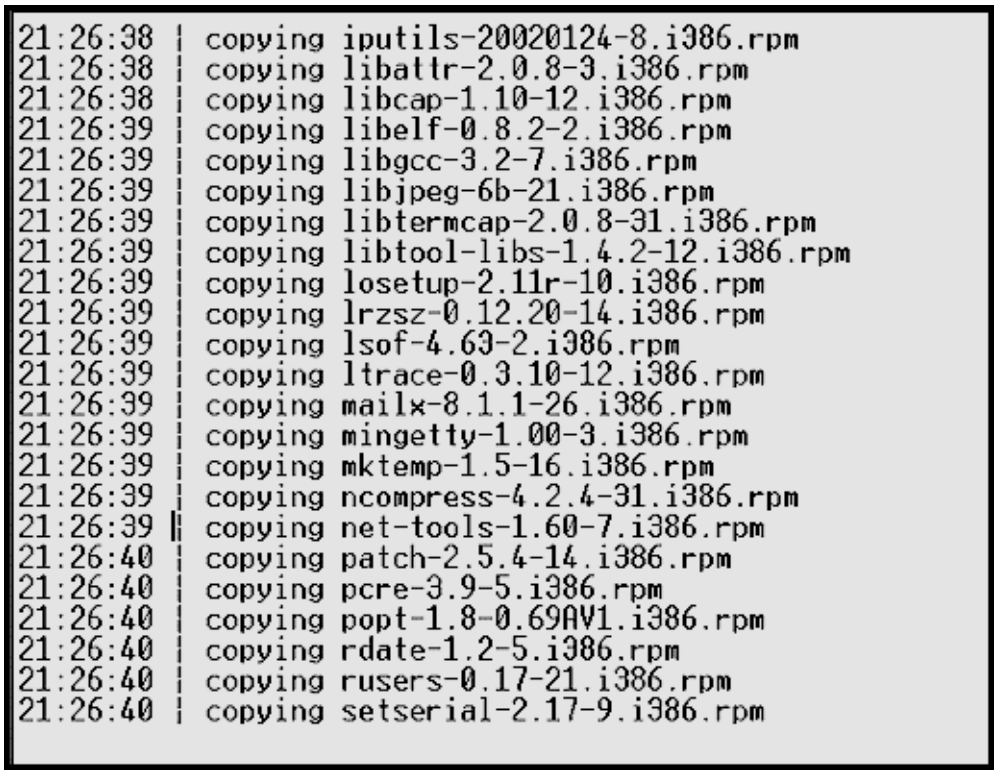
   At this point, the following processes are initiated:

   a. The S8300 hard drive is 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



   These processes take 15–30 minutes.

   d. If IA770 installation has been selected, it is then installed.

When the media server is ready to reboot, the following screen flashes for about 5 seconds.

Software and firmware update reminder

When the installation is complete, the CD drive door opens and the system reboots automatically. The reboot takes 1–3 minutes.

In the event you used the laptop TFTP server and you have a problem with power and the S8300 does not reboot, there are two methods of recovery:

- Use the USB CD-ROM to plug into the S8300 and repeat the remastering process using the Server CD.
- Arrange access to another hard drive (comcode 700307028) should it be necessary to perform the TFTP remaster procedure on it.

About the Avaya Installation Wizard

You can use the Avaya Installation Wizard (IW) to perform all of the following tasks:

- Configure the S8300 Media Server
- Configure the G700 Media Gateway
- Install new firmware on the G700

Configure the S8300 Media Server

The IW accomplishes the following tasks:

- Verifying software version
- Setting the media server's time, date, and time zone
- Installing Communication Manager service pack files, if any
- Configuring the S8300 Media Server
- Configuring the Stack Master/IP routing

- Configuring Optional Services (UPS, DNS, NTP, INADS)
- Creating Translations
- Installing license and authentication files

Enabling Network Time Servers

Important:

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

Enabling Network Time Protocol allows you to specify one, two, or three network time servers to provide accurate time-of-day data to the clocks on the media servers. The network time servers, in turn, get their source timing from one of several highly accurate time services available on the Internet.

To use a network time server, the NTP service must be enabled. The Avaya Installation Wizard prompts for enabling the NTP service.

If you are not using the Installation Wizard, or if you want to see if NTP is enabled, follow these steps:

1. Open the Maintenance Web Interface
2. Click on the **Firewall** link under Security.
3. Enable **ntp 123/udp** in the "Output from Server" column by clicking on the checkbox.

Note:

It is not necessary to enable the "Input to Server" ntp service but if it is already enabled, you don’t have to disable it.

In the next section, Using the Avaya Installation Wizard (IW) on page 148, the Avaya Installation Wizard prompts for information about network time servers. When prompted, enter the DNS name or IP address for the primary (and secondary and tertiary, if any) network time server. If you enter a DNS name instead of an IP address for the network time server, the DNS server IP address must be specified. You are prompted for this information by the Installation Wizard.

If you are not using the Installation Wizard, the network time servers can be configured using the Configure Server function on the Maintenance Web Interface.

For detailed information about NTP, see RFC 958.

Configure the G700 Media Gateway

This section describes the procedures for configuring the G700 Media Gateway. The IW performs the following tasks:

- Assigning the IP addresses of the G700 Media Gateway components
- Setting up the controller list for the G700
- Setting the Link Loss transition points

However, the following task must be performed manually, if necessary:

- Configuring an X330 Expansion Module (if necessary)

Install new firmware on the G700

The IW performs the procedures to install firmware on the G700 Media Gateway processors and media modules. These procedures include:

- 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

The G700 is shipped with firmware installed for all G700 components. When you install Communication Manager software, the latest versions of the G700 firmware are copied to the S8300 tftpboot directory. The IW displays the firmware versions resident on the S8300 hard drive and the available versions, and allows you to request a firmware upgrade for any component whose resident firmware is not the latest.

The following tasks must be performed manually:

Setting rapid spanning tree on the network

Installing IA770 service pack files, if any

Electronic worksheets and templates

To allow the IW to automatically configure and install the system, obtain the following files from the project manager and load them onto your laptop:

- Electronic Pre-Installation Worksheet
- Name and Number List (S8300 with a G700 or G350 only)
- Custom Template (S8300 with a G700 or G350 only)

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 (S8300 with G700 or G350 only)

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/avayaiw 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 (S8300 with G700 or G350 only)

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

Obtaining further information on the Avaya Installation Wizard

Additional information on the Avaya Installation Wizard, including:

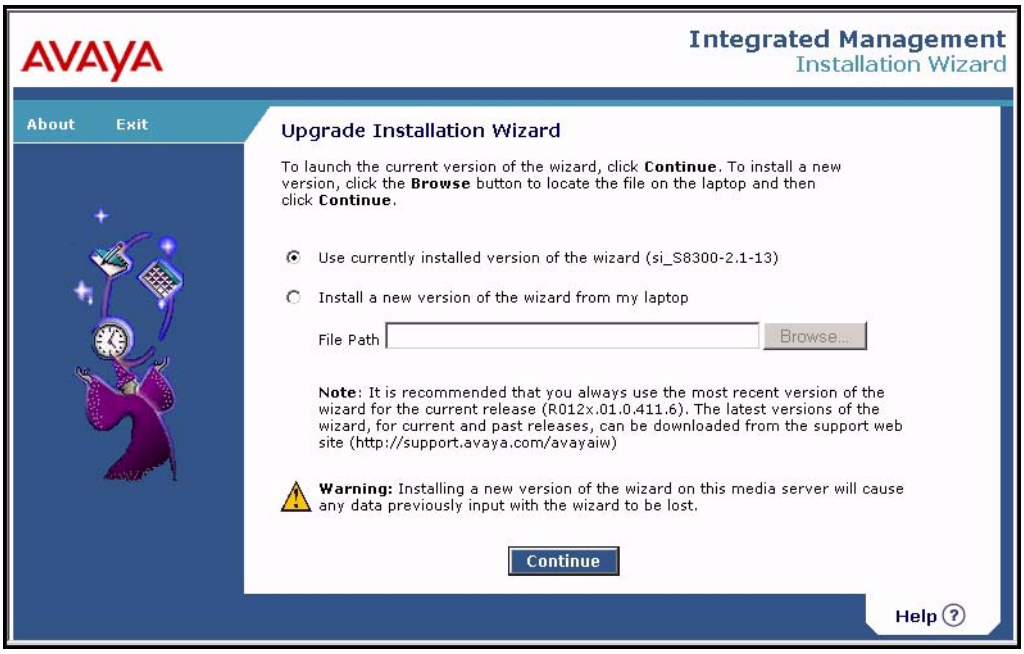
- Tasks to complete before going onsite
- Installing hardware
- Setting up the IW
- Overview of IW tasks

can be found in *Job Aid: Avaya Installation Wizard, 555-245-754*.

Using the Avaya Installation Wizard (IW)

From the Maintenance Web Interface, launch the Avaya Installation Wizard. The **Upgrade Installation Wizard** screen displays. You can use the currently installed version of the IW, or you can choose to install a new version of the IW from your laptop.

Upgrade Installation Wizard screen

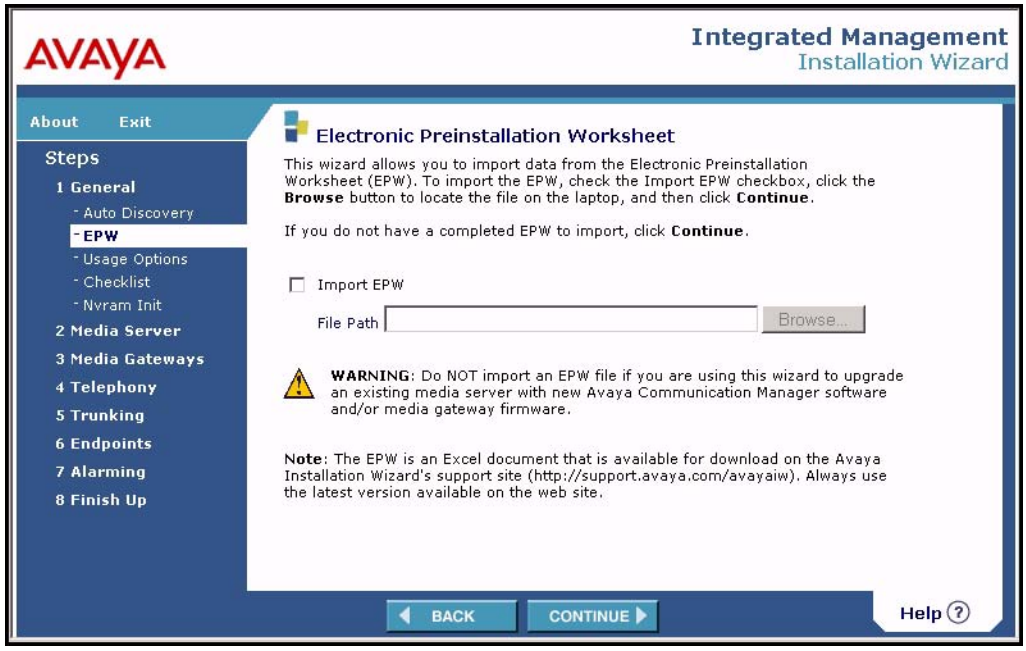


When you are finished with the Upgrade Installation Wizard screen, click **Continue**. Following brief **Overview** and **Auto Discovery** screens that display system data for the installation, such as:

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

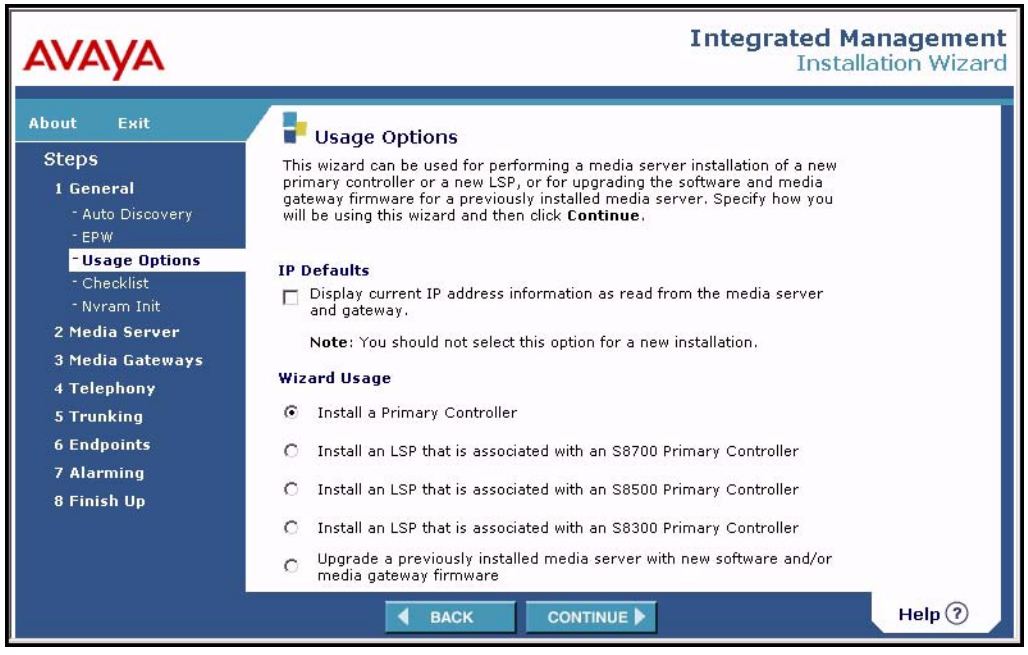
click the **Continue** button, and the **Electronic Preinstallation Worksheet** screen displays.

Electronic Preinstallation Worksheet screen



If you had prepared the EPW beforehand and loaded it onto your laptop, you could import installation and configuration data into IW at this time. When you are finished with this screen, click the **Continue** button. The **Usage Options** screen displays.

Usage Options screen



You can choose any of several **Wizard Usage** options. For a new installation, you could select the **Install a Primary Controller** radio button if the S8300 were going to be operated in primary controller mode; or you could select one of the LSP options, depending on the type of primary controller the system has. Leave the **IP Defaults** checkbox unchecked.

Note:

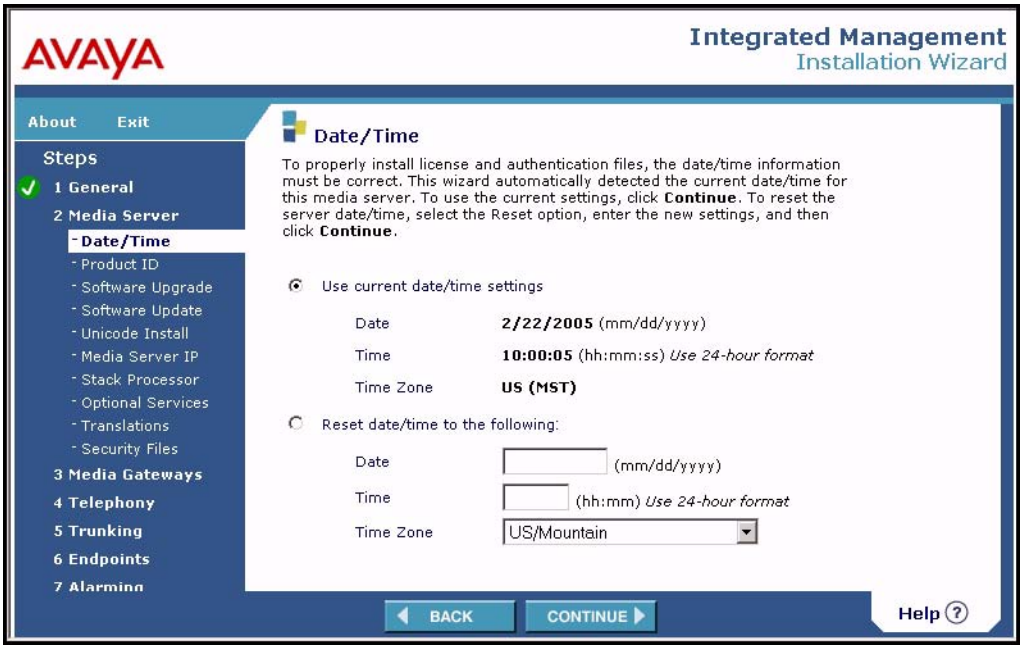
One of the options is an upgrade of a previously installed media server with new software and/or media gateway firmware. This is the option you would choose in an upgrade-only scenario.

When you are finished with this screen, 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 **`nvram 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.

Click **Continue** to begin the **Media Server** tasks. The first screen to display is the **Date/Time** screen.

Date/Time screen



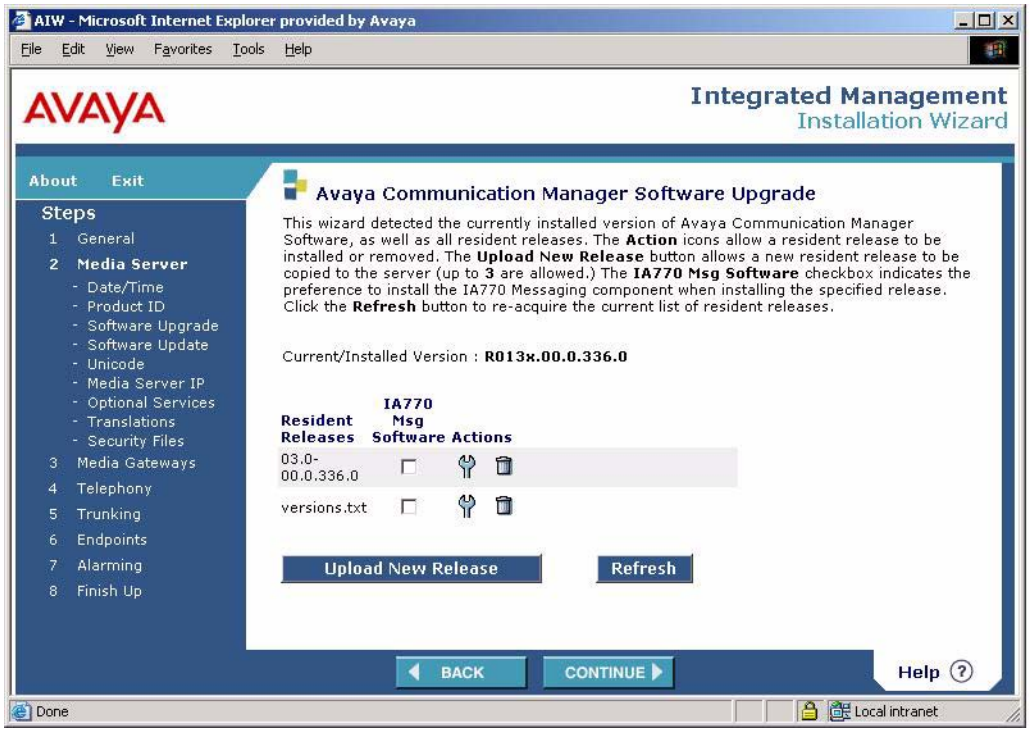
In this screen, you can choose to use the current date and time information that the IW detects on the S8300, or you can reset the date, time, and time zone. When you are finished, click **Continue**.

The IW proceeds to display the following screens, some or all of which the EPW or you may fill in, depending on your planning documentation:

- Product ID - a product ID, obtained from Avaya's Automatic Registration Tool (ART)
- Software Upgrade - install a version of Communication Manager, either a new version, an upgrade, or use a currently installed version

  The **Avaya Communication Manager Software Upgrade** screen displays.

Avaya Communication Manager Software Upgrade screen



The **Upload New Release** button allows a new resident release to be copied to the server. The **IA770 Msg Software** checkbox indicates your preference to install the IA770 Messaging component, when installing the specified release.

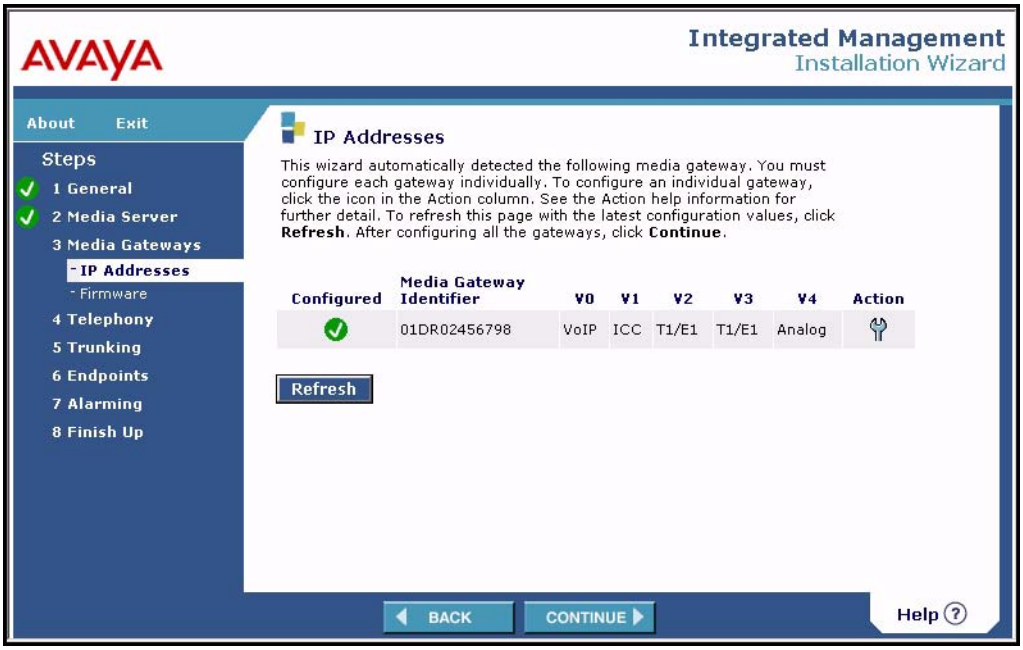
- Software Update - remove and/or install software service packs
- Unicode Install - install Standard and Custom Unicode phone message files that provide unicode messages for display sets that are in the desired unicode language format
- Media Server IP - configure the S8300 Media Server to access the LAN (EPW fills this in)
- Stack Processor - configure the P330 Stack Processor to access the LAN, and configure IP routing (EPW fills this in)
- Optional Services - you can identify any or all of these optional services for this installation:
  - Uninterruptible Power Supply (UPS) - identify the UPS system on the network for this solution

- Domain Name Service (DNS) - identify the DNS servers on the customer network
- Network Time Protocol (NTP) - select the NTP option for time-of-day (TOD) synchronization for this solution. Depending on the solution, additional screens allow you to define NTP server IP addresses, trusted keys (if necessary), multicast client support, and other support.
- Remote access/INADS support - configure INADS remote support information obtained from the ART tool.

- Translations - use the IW to create basic translations, or defer translations until after the installation is completed (using SAT, ProVision, ASA, or another Integrated Management tool)
- Security Files - install license and authentication files for this solution from the laptop

When you are finished with the **Media Server** screens, click **Continue**. The **Media Gateway** screens display. The first of these is the **IP Addresses** screen.

IP Addresses screen

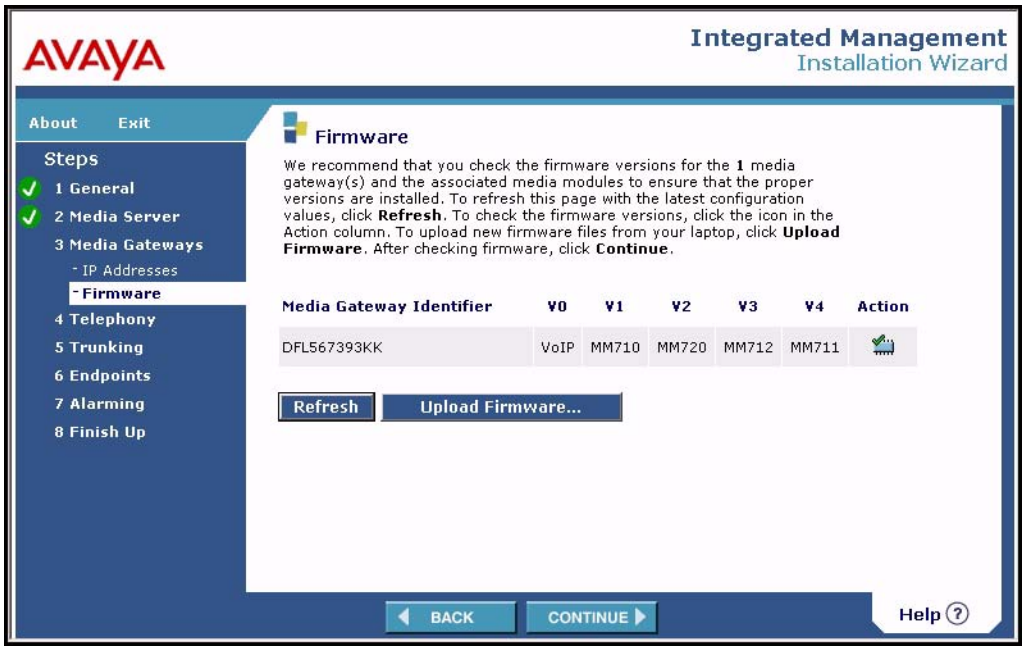


The IW identifies the Media Gateway serial number and all media modules present. When configuring a new gateway, click on the **Action** Icon. This opens four additional screens, which allows you or the EPW to configure the following:

- Media Gateway Processor- identifies the Media Gateway Processor (MGP) to the network
- Add IP Route - configures additional IP routes on the network
- Media Gateway Controller List - configures the MGC list and sets LSP transition points. On this screen, a PING test to each of the controllers in the MGC list can be conducted.
- VoIP Modules - configures all VoIP engines on the gateway

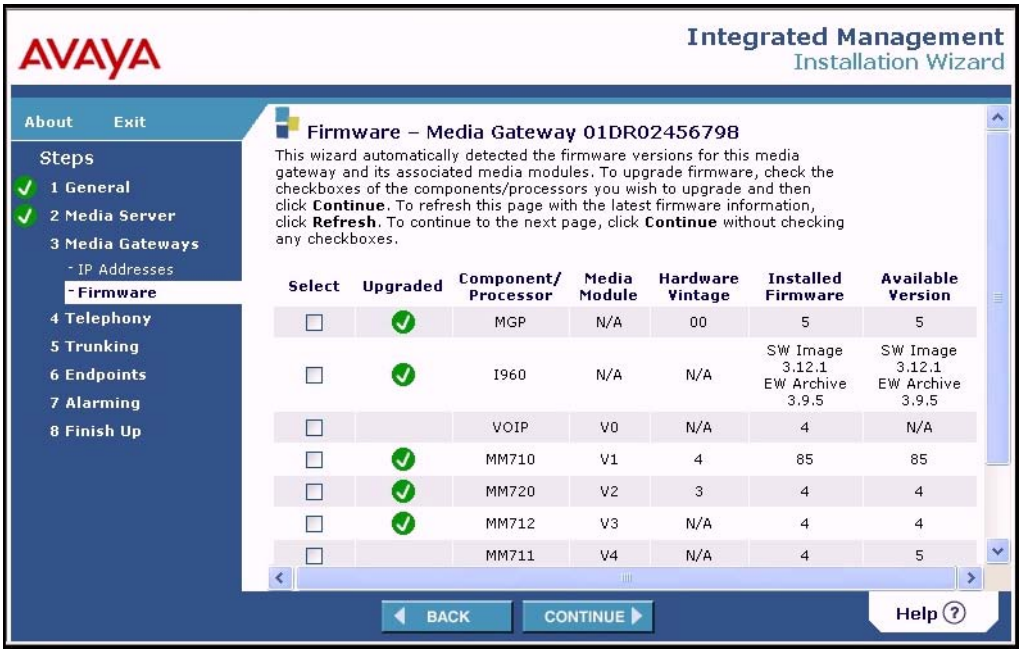
After returning to the **IP Addresses** screen, a green-circled checkmark signifies that the Media Gateway has been configured. Click **Continue**. The **Firmware** screen displays.

Firmware screen



To check the firmware versions, click the **Action Icon**. The **Firmware - Media Gateway <*serial number*>** screen displays.

Firmware - Media Gateway <*serial number*> screen



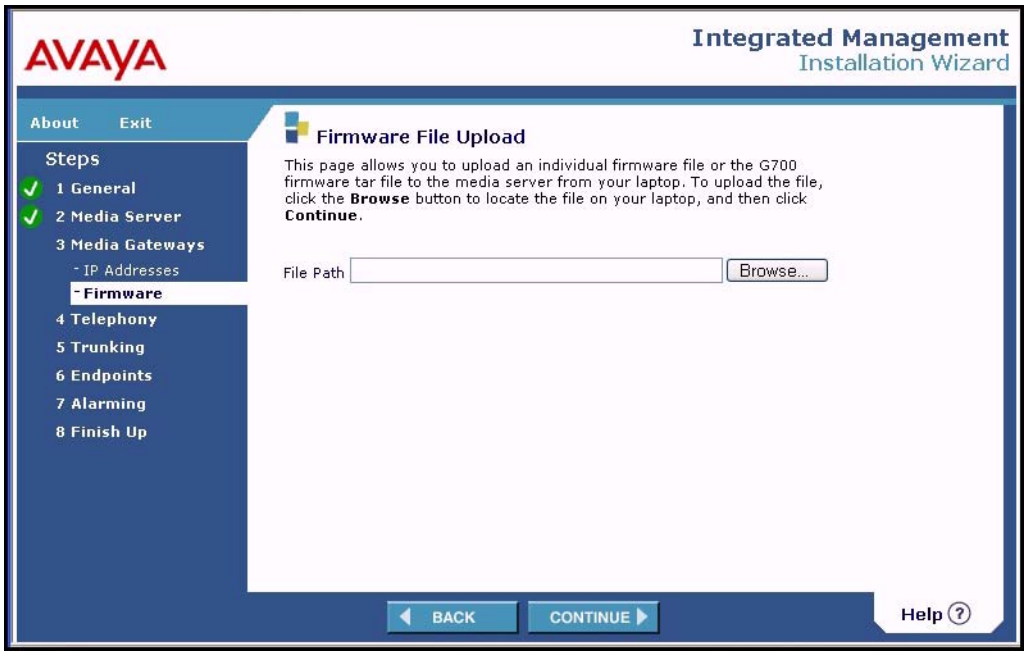
This screen shows for both the Media Gateway and its media modules the firmware resident on the component and the available versions of firmware present on your laptop.

Note:

New firmware can be uploaded from the previous screen. Click **Back** to return to that page.

From the Firmware screen, click **Upload firmware.** The **Firmware File Upload** screen displays.

Firmware File Upload screen



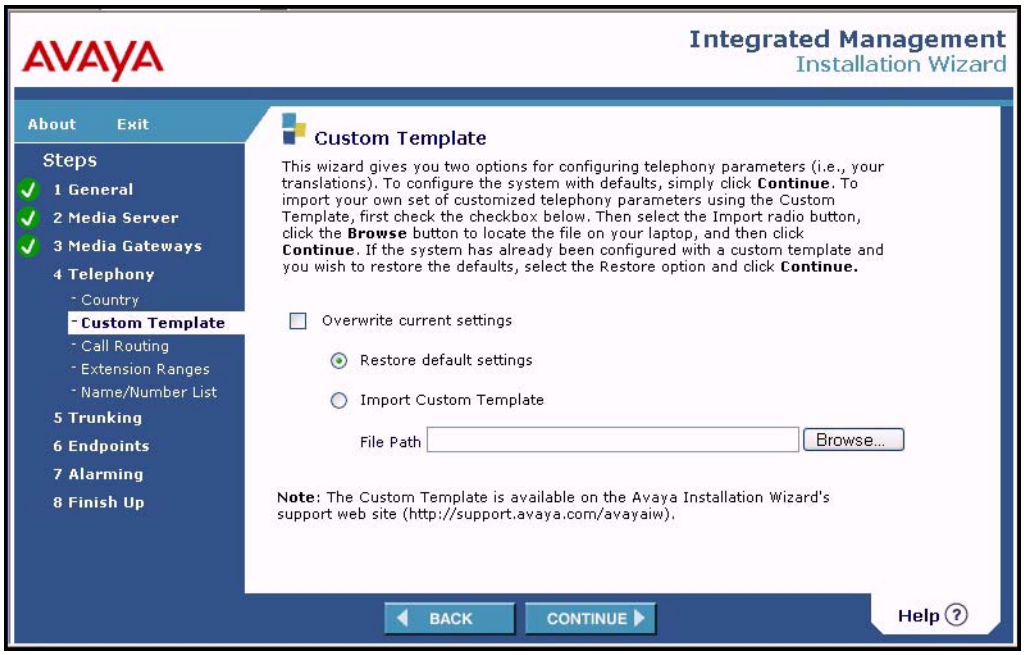
You must upload one firmware file at a time. Browse to the file location on your laptop and then click **Continue**. A green-circled checkmark next to the component's name on the **Firmware - Media Gateway <*serial number*>** screen signifies that the component firmware has been successfully uploaded. When you are finished, click **Continue**. This returns you to the **Firmware** screen. If you have finished checking firmware on the **Firmware** screen, click **Continue**.

Several screens related to **Telephony** display, including:

- Country - select the country for the location of this installation
- Custom Template - options for configuring telephony parameters
- Call Routing - specify call routing information
- Extension Ranges - specify the extension ranges the S8300 Media Server will support
- Name/Number List - import file with name/number list and user information

Following the **Country** screen, the **Custom Template** screen displays.

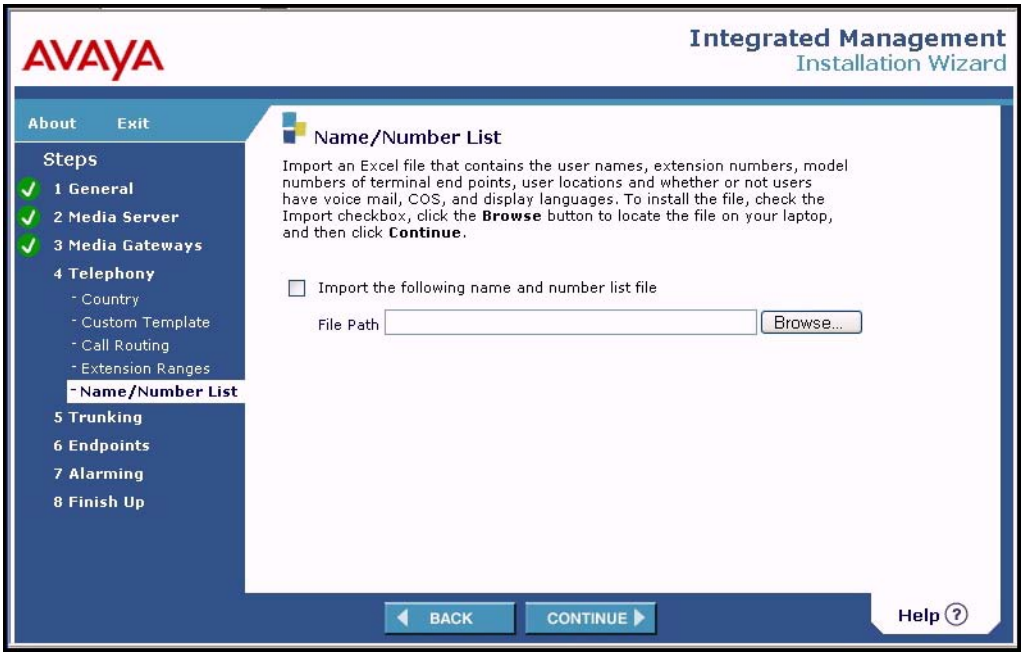
Custom Template screen



You can configure the system with default telephony settings, or you can configure your own set of custom telephony parameters by importing the Custom Template. Select the Import Custom Template radio button, then browse to the location on your laptop where you have stored the Custom Template, and click **Continue**.

After the **Call Routing** and **Extension Ranges** screens, the **Name/Number List** screen displays.

Name/Number List screen



You can import an Excel file that contains user names, extension numbers, and other user data. Check the **Import the following name and number list file** checkbox, browse to the file's location on your laptop, and click **Continue**.

You can choose to exit the IW to perform manual tasks at any time. A dialog box displays with the following message:

If you choose to exit now, this wizard will save the information that you have entered. The next time you launch this wizard, you will have the option to continue where you left off or start over.

Installing IA770 service pack 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.

To obtain the post-upgrade service pack file and documentation

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.

7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 software.

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).

Administer Communication Manager

Important:

The administration procedures in this section are performed manually in a SAT session 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 S8500 or S8700-series.

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 S8500 or S8700 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 S8500 or S8700 primary controller on page 166 if the primary controller is an S8500 or S8700-series.

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
- Administering the LSP Form

CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Telnet to the S8300, log in, and open a SAT session (type **sat** or **dsat**).
2. At the SAT prompt, type **`reset system 4`**

   The system reboots.
3. 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
 DiffServ/TOS PARAMETERS              Use Default Server Parameters? y
 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 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 Ehternet Port?
       Nework Region: 1
```

2. The field **Enable Ethernet Port?** should indicate `y` (yes)**.** The **Node Name** should be the IP address of the S8300 media server.

Administering the LSP Form

If the primary controller 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** screen, their status can be viewed with the **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **LSP** screen.

To add LSP names to the LSP screen

1. At the S8300 SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?        Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                      out-of-service
3      _____________                      out-of-service
4      _____________                      out-of-service
5      _____________                      out-of-service
6      _____________                      out-of-service
7      _____________                      out-of-service
8      _____________                      out-of-service
9      _____________                      out-of-service
10     _____________                      out-of-service
11     _____________                      out-of-service
12     _____________                      out-of-service
13     _____________                      out-of-service
14     _____________                      out-of-service
15     _____________                      out-of-service
16     _____________                      out-of-service
```

2. Enter the node name for each LSP supported by the primary controller and submit the form.

Skip to Administering the Media Gateway on page 173.

Administering an S8500 or S8700 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 S8500 or S8700 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 160 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
- Administering the LSP Form

Note:

For information on installing the CLAN boards on the S8500 or S8700 port networks and complete information on installing an S8700 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 S8700. For information on how to upgrade the firmware on the S8700, please see the section "Upgrade Firmware in Selected Port Cabinet Packs" in *Upgrading the Avaya media server Configuration* in the S8700 documentation portion of this documentation CD, "*Avaya S8300, S8500, and S8700 media server Library CD*," 555-233-325."

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 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 with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700 port networks, though they may also have the same network region.

The G700, in this case, 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 S8500 or S8700. The G700 network region may also differ because of the nature of the endpoints connected to it.

To define IP network regions for the G700 and CLAN board(s)

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. 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 S8500 or S8700 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:                  Home Domain:
    Name:
                                    Intra-region IP-IP Direct Audio: yes
AUDIO 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
 DiffServ/TOS PARAMETERS           Use Default Server Parameters? y
 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. 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 S8500 or S8700 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                              Page   3 of 19
                 Inter Network Region Connection Management

src dst   codec  direct                                      Dynamic CAC
rgn rgn    set    WAN   WAN-BW-limints  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 S8500 or S8700 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
LSP NAMES IN PRIORITY ORDER
1   node-10-LSP______
2   _________________
3   _________________
4   _________________
5   _________________
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 S8500 or S8700 port network CLAN boards

Note:

This should have already been established as a part of normal S8500 or S8700 installation.

1. Type **`change ip-interfaces`** to open the **IP Interfaces** screen.

IP Interfaces Screen

```
change ip-interfaces procr                                    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 Ehternet Port? y
       Nework Region: 1
                VLAN: 0

Number of CLAN Sockets Before Warning: 400
```

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 "*Administration for Network Connectivity for Avaya Communication Manager, 555-233-504"*.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
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 8: IP interfaces field descriptions (continued)

Field	Conditions/Comments
VLAN	The VLAN number assigned to the C-LAN, if any.
Number of CLAN Sockets Before Warning	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.

2 of 2

3. Close the screen.

Administering the LSP Form

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 **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

To add LSP names to the LSP screen

1. At the SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                          Page   1 of   16
                        LOCAL SURVIVABLE PROCESSOR
Number NAME          IP Address             Service      Translations
                                             State?        Updated
1      node-10-LSP_  192.168.1.50           in-service   14:21 5/4/2003
2      _____________                      out-of-service
3      _____________                      out-of-service
4      _____________                      out-of-service
5      _____________                      out-of-service
6      _____________                      out-of-service
7      _____________                      out-of-service
8      _____________                      out-of-service
9      _____________                      out-of-service
10     _____________                      out-of-service
11     _____________                      out-of-service
12     _____________                      out-of-service
13     _____________                      out-of-service
14     _____________                      out-of-service
15     _____________                      out-of-service
16     _____________                      out-of-service
```

2. Enter the node name for each LSP supported by the primary controller.
3. Submit the form.

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 and 250 for an S8500 or S8700).

   The S8300 displays the **Media Gateway** screen.

Add media gateway Screen

```
add media-gateway 1                                      Page  1 of 1
                           MEDIA GATEWAY
        Number: 1                              IP Address: 135.9.41.150
          Type: g700                FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                      MAC Address:
     Serial No: 012X06230551                 Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? n                  Controller IP Address:
                                                Site Data:
     Slot    Module Type                Name
      V1:
      V2:
      V3:
      V4:


      V8:
      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 S8500 or S8700 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                              IP Address: 135.9.41.150
          Type: g700                 FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                     MAC Address: 00:04:0d:02:06:ca
     Serial No: 012X06230551                 Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? y                   Controller IP Address: 135.9.41.146
                                                Site Data:
     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/          IP Address/          Type   NetRgn
Reg?
                        FW Ver/HW Vint      Cntrl IP Addr

1        LabA           01DR07128730      135.177.49.57        g700     1
y
                        21 .13 .0  /0     135.177.49.59
2        Data MG2       02DR01130356      135.177.49.90        g350     1
n
                        11 .2  .0  /0     135.177.49.40
```

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 S8500 or S8700 system, this is a CLAN address; 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 S8700 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 looses 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 S8500 or S8700 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 S8500 or S8700 alarms to notify the customer and services personnel that the network connection between the S8500 or S8700 and G700 has problems. If control passes to the LSP, the LSP’s license allows it to support the G700 endpoints for up to 10 days, within which the network problems should be resolved.

The customer must pass control back to the S8500 or S8700 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, in this case the S8500 or S8700.

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.

Backing up the system

To back up the system

1. Make sure you have the IP address of the customer's FTP 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**, 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 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 site may have a different convention.

- **Host name**

  Enter the DNS name or IP address of the FTP 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 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 *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532.

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

This chapter covers the 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 Manger. 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 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.

How is normal access to the S8300 and G700 provided

You can access the S8300 and G700 in several ways with either a direct connection or LAN connection.

Note:

Before the Upgrade Tool can be used to upgrade software on an LSP or firmware on a G700, as summarized below, the LSP must be administered on the primary controller.

Connecting directly to a target S8300

If you are at the location of the target S8300 (primary or LSP), you can connect directly to the S8300 Services port.

To install or upgrade directly

1. Install the S8300 software by:
   - Opening the Web interface and using the Avaya Installation Wizard

     or,
   - Opening the Web interface and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or the Upgrade Tool

     or,
   - Opening a telnet session to the S8300, and then telnet to the P330 stack processor

Connecting directly to the remote primary server (S8300, S8500, or S8700)

In this case, the target S8300 is an LSP. If you are at the location of the remote primary server, you can connect directly to the remote server's Services port.

To install or upgrade the target LSP remotely

1. Install the S8300 (LSP) software by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool

     or,

- Opening a telnet session to the primary server and then telnet to the P330 stack processor and perform the installation commands

Note:

For direct connections, the TFTP server must be on the Customer LAN, not on your laptop.

Connecting using the customer's LAN

If you can connect to the customer's LAN, you can:

1. Install the S8300 software by:
   - Opening the Web interface on the S8300 and using the Avaya Installation Wizard

     or,

   - Opening the Web interface on the S8300 and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface on the primary server and using the Avaya Installation Wizard or Upgrade Tool

     or,

   - Opening a telnet session to the P330 stack processor and perform the installation commands

Note:

For LAN connections, the TFTP server can be your laptop or a customer computer on the LAN.

See About connection and login methods on page 47 for details on how physically to connect and log into the G700.

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.

Collecting Installation Information

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
- Type of system
- Equipment needed

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.

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, 1.3 to 2.0), you will need the serial number of the G700. To get this number, ask the customer's administrator to log in to the S8300 web page and select **View License Status** from the main menu to display the serial number.

For a new installation, 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.

Installing the Gateway Installation Wizard

To obtain the 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-3.0-1.exe**).
4. Save it to a directory on your laptop.
5. Click on the GIW Readme file (for example, **GIW-3.0-1.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 9.

Note:

The latest firmware versions may different from those listed in Table 9. 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.

Table 9: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_0_17.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.0.4.exe
G700 Media Gateway	mgp<version id>	mgp_21_16_0.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v43.fdl
8-port DCP Media Module	mm712<version id>	mm712v5.fdl
		1 of 2

Table 9: Firmware file formats (continued)

Component	Firmware Version Format	Example
24-Port DCP Media Module	mm717<version id>	mm717v2.fdl
8-port/trunk Analog Media Module	mm711<version id>	mm711h20v60.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v60.fdl
T1/E1 Media Module	mm710<version id>	mm710v9.fdl
8-port BRI Media Module	mm720<version id>	mm720v4.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:

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

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)

Install firmware on the G700 and media modules

The Avaya Gateway Installation Wizard (GIW) can perform the installation of new firmware on the G700 and media modules automatically. Before installing new firmware on the G700 processors and media modules, the GIW:

- Accesses the P330 Stack Processor
- Verifies the contents of the tftpboot directory

Following this the GIW performs the 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

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://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.

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 S8500 or S8700-series.

Perform one of the following two administration procedures in this section:

- Administering an S8300 primary controller
- Administering an S8500 or S8700-series primary controller

Administering an S8300 primary controller

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
- Administering the LSP Form

CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Telnet to the S8300, log in, and open a SAT session (type **sat** or **dsat**).
2. At the SAT prompt, type **`reset system 4`**

   The system reboots.
3. 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
 DiffServ/TOS PARAMETERS            Use Default Server Parameters? y
 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 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 Ehternet Port?
       Nework Region: 1
```

2. The field **Enable Ethernet Port?** should indicate y (yes)**.** The **Node Name** should be the IP address of the S8300 media server.

Administering the LSP Form

If the primary controller 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** screen, their status can be viewed with the **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **LSP** screen.

To add LSP names to the LSP screen

1. At the S8300 SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?         Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                      out-of-service
3      _____________                      out-of-service
4      _____________                      out-of-service
5      _____________                      out-of-service
6      _____________                      out-of-service
7      _____________                      out-of-service
8      _____________                      out-of-service
9      _____________                      out-of-service
10     _____________                      out-of-service
11     _____________                      out-of-service
12     _____________                      out-of-service
13     _____________                      out-of-service
14     _____________                      out-of-service
15     _____________                      out-of-service
16     _____________                      out-of-service
```

2. Enter the node name for each LSP supported by the primary controller and submit the form.

Skip to Administering the Media Gateway on page 205 to continue.

Administering an S8500 or S8700-series primary controller

Complete the procedures in this section if the primary controller for the G700 you are installing is an S8500, S8700 or S8710. If the primary controller is an S8300, you should have completed the procedures in Administering an S8300 primary controller on page 193.

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
- Administering the LSP Form

Note:

For information on installing the CLAN boards on the S8500 or S8700 port networks and complete information on installing an S8700 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 S8700. For information on how to upgrade the firmware on the S8700, please see the section "Upgrade Firmware in Selected Port Cabinet Packs" in *Upgrading the Avaya media server Configuration* in the S8700 documentation portion of this documentation CD, "*Avaya S8300, S8500, and S8700 media server Library CD*," 555-233-325."

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 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 with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700 port networks, though they may also have the same network region.

The G700, in this case, 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 S8500 or S8700. The G700 network region may also differ because of the nature of the endpoints connected to it.

To define IP network regions for the G700 and CLAN board(s)

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. 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 S8500 or S8700 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:                  Home Domain:
    Name:
                                   Intra-region IP-IP Direct Audio: yes
AUDIO 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
 DiffServ/TOS PARAMETERS           Use Default Server Parameters? y
 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. 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 S8500 or S8700 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                                Page   3 of 19
                 Inter Network Region Connection Management

src dst   codec  direct                                    Dynamic CAC
rgn rgn    set    WAN   WAN-BW-limints  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 S8500 or S8700 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
LSP NAMES IN PRIORITY ORDER
1   node-10-LSP______
2   _________________
3   _________________
4   _________________
5   _________________
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 S8500 or S8700 port network CLAN boards

Note:

This should have already been established as a part of normal S8500 or S8700 installation.

1. Type **`change ip-interfaces`** to open the **IP Interfaces** screen.

IP Interfaces Screen

```
change ip-interfaces procr                                    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 Ehternet Port? y
       Nework Region: 1
               VLAN: 0

Number of CLAN Sockets Before Warning: 400
```

2. Complete the fields as described the in Table 10.

Table 10: 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 "*Administration for Network Connectivity for Avaya Communication Manager, 555-233-504"*.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
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.
Number of CLAN Sockets Before Warning	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.

3. Close the screen.

Administering the LSP Form

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 **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

To add LSP names to the LSP screen

1. At the SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?        Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                       out-of-service
3      _____________                       out-of-service
4      _____________                       out-of-service
5      _____________                       out-of-service
6      _____________                       out-of-service
7      _____________                       out-of-service
8      _____________                       out-of-service
9      _____________                       out-of-service
10     _____________                       out-of-service
11     _____________                       out-of-service
12     _____________                       out-of-service
13     _____________                       out-of-service
14     _____________                       out-of-service
15     _____________                       out-of-service
16     _____________                       out-of-service
```

2. Enter the node name for each LSP supported by the primary controller.
3. Submit the form.

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 and 250 for an S8500 or S8700).

   The S8300 displays the **Media Gateway** screen.

Add media gateway Screen

```
add media-gateway 1                                     Page  1 of 1
                           MEDIA GATEWAY
        Number: 1                              IP Address: 135.9.41.150
          Type: g700                 FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                     MAC Address:
     Serial No: 012X06230551                 Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? n                   Controller IP Address:
                                                Site Data:
     Slot    Module Type                Name
      V1:
      V2:
      V3:
      V4:


      V8:
      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 S8500 or S8700 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                              IP Address: 135.9.41.150
          Type: g700                FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                    MAC Address: 00:04:0d:02:06:ca
     Serial No: 012X06230551                Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? y                  Controller IP Address: 135.9.41.146
                                                Site Data:
     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/        IP Address/        Type   NetRgn
Reg?
                      FW Ver/HW Vint    Cntrl IP Addr

1        LabA         01DR07128730     135.177.49.57       g700    1       y
                      21 .13 .0  /0    135.177.49.59
2        Data MG2     02DR01130356     135.177.49.90       g350    1       n
                      11 .2  .0  /0    135.177.49.40
```

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 S8300A to R3.0 using the Wizards

About upgrading an existing S8300A to R3.0

This chapter covers the procedures to upgrade Communication Manager software to release 3.0 on an installed Avaya S8300 Media Server, version A. The current Communication Manager release can be any pre-2.1 release. These procedures require replacing version A of the S8300 with version B. 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. If the currently installed S8300 is version B, follow the upgrade procedures in Chapter 6: Upgrading an existing S8300B to R3.0 using the Wizards.

The B version of the S8300 shows a “B” on the faceplate (see Figure 17: S8300B version faceplate on page 211) — the version is not indicated on the faceplate of the A version.

Figure 17: S8300B version faceplate

The S8300 version can also be determined with the SAT command, `list config all`. The B version is listed as **S8300B**. 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 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. 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.

Note:

Because of the replacement of the S8300A and the reformatting of the S8300B hard drive, the Avaya Installation Wizard (IW) cannot support upgrades of Communication Manager to release 3.0 when starting with the S8300A version. However, the IW can still be used to configure the S8300B after the remastering process, and the IW or the Upgrade Tool can still be used for the media gateway and media module firmware upgrades.

Release 3.0 upgrade scenarios

The upgrade procedures are slightly different depending on the upgrade scenario. The main differences between the scenarios are summarized in Table 11 and are noted in the detailed procedures.

Table 11: Release 3.0 upgrade scenarios

Upgrade From	S8300 B Hard Drive has Remastering Software Only	S8300 B Hard Drive has R2.x Software Installed
R 1.x	Linux Migration backup Remaster and upgrade View/Restore Data	Linux Migration backup Upgrade View/Restore Data
R 2.x	Backup Now Remaster and upgrade View/Restore Data	Backup Now Upgrade View/Restore Data
	Move hard drive from A to B Upgrade	

The unshaded cells in this table are the most common and recommended upgrade scenarios. The shaded cells are scenarios that are unlikely or not recommended.

The new S8300B media server will normally not have Communication Manager software installed on it. If it does, remastering the hard drive is still recommended but could be replaced with a standard upgrade.

If the current system has a 2.0.x release of Communication Manager installed, it is possible to move the hard drive from the S8300A to the S8300B and then upgrade to 3.0. This saves a few steps but it is not recommended for the following reasons:

- If the S8300 A hard drive is not moved, it provides a means to quickly revert to the original configuration, if necessary.
- Hardware could be damaged in the process of changing hard drives.
- Only the Fujitsu hard drives can be moved.
- The hard drives on the S8300B have a larger capacity than the hard drives on the S8300A. This larger capacity is not needed for R 3.0 but may be needed in the future.

Accessing the Server CD

The R3.0 Communication Manager software and other files needed for the R3.0 upgrade are on the Server CD that you take to the customer site. You can make the Server CD available to the upgrade process in one of two ways:

- ***Recommended:*** Place the CD in the CD-ROM drive on the technician's laptop. This method requires that the Avaya TFTP Server software (available at support.avaya.com) is installed on the technician's laptop. In addition, this method requires that the S8300B ***does not*** have Communication Manager software installed on its hard drive.

  or,

- Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate. This method works whether or not Communication Manager software is installed on the S8300B hard drive.

  Important:
  Before you go to the site, either you must have the TFTP server installed on your laptop (recommended), or you must have an external USB CD-ROM drive.

  The new S8300B will normally not have Communication Manager software installed on its hard drive. You should check the S8300B that you will be installing before going to the site to determine whether you need to have the external USB CD-ROM drive.

  - If software is not installed, the hard drive label is "S8300B Hard Drive Without CM Software."
  - If software is installed, the label indicates the software release. In this case, you must use the external USB CD-ROM drive because the TFTP server on your laptop will not work.

This chapter describes the upgrade procedure with the TFTP Server software installed on the laptop and using the laptop CD-ROM drive as source of the upgrade software. For instructions on obtaining and installing the Avaya TFTP Server, see Appendix D: Install the Avaya TFTP server.

Accessing the S8300

To access the S8300 on-site, you normally connect the technician's laptop directly to the Services port on the S8300 using a crossover cable. See About connection and login methods on page 47 for instructions on accessing the S8300 and G700.

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.

Do the following procedures:

- Installing TFTP server or obtaining USB CD-ROM drive on page 215

  Important:
  If the new S8300B that you will be installing has Communication Manager software installed on its hard drive, you must use an external USB CD-ROM drive instead of the TFTP server on your laptop. See Accessing the Server CD on page 213 for more information.

- Filling in the EPW, if upgrading from release 1.1 on page 215
- Planning forms provided by the project manager on page 215
- Getting the serial number of the G700, if necessary on page 216
- Checking the number of allocated ports on page 216
- Identifying the FTP server for backing up data on page 216
- Obtaining S8300 software and G700 firmware on page 217
- Obtaining service pack files on page 218
- If using IA770, checking stored messages size, obtaining service pack (or RFU) and language files on page 219
- Completing the RFA process (obtaining license and authentication files) on page 221

Installing TFTP server or obtaining USB CD-ROM drive

Upgrading Communication Manager on an S8300 to release 3.0 normally requires remastering the S8300B hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on:

- An external USB CD-ROM drive, or
- The laptop, if a TFTP server is installed

You must have either the Avaya TFTP server software installed on your laptop or take a USB CD-ROM drive to the site. If you do not already have the Avaya TFTP server installed on your laptop, you can obtain the software from the Avaya Support website and install it as described in Appendix D: Install the Avaya TFTP server.

Important:
If the new S8300B that you will be installing has Communication Manager software installed on its hard drive, you must use an external USB CD-ROM drive instead of the TFTP server on your laptop. See Accessing the Server CD on page 213 for more information.

Collecting upgrade information

Filling in the EPW, if upgrading from release 1.1

If you are upgrading from release 1.1, you will need to do a complete configuration of the S8300B after the upgrade to release 3.0. 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/avayaiw/ 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.

Planning forms provided by the project manager

The Project Manager should provide you with forms that contain all the information needed to prepare for this installation. The information includes IP addresses, subnet mask addresses, logins, passwords, people to contact, the type of system, and 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.

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 often 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 3.0 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.

Identifying the FTP server for backing up data

During the installation and upgrade procedures, you will need to back up the system data to an FTP server. Normally, you will use an FTP server on the customer's LAN for backups.

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

Check with your project manager or the customer for this information.

Important:
Before going to the customer site, make sure that you can use a customer server for backups.

Obtaining S8300 software and G700 firmware

The file containing the software for the S8300 has a *.tar extension and contains both the S8300 software and the G700 and media module firmware. The *.tar file is on a CD-ROM that you take to the site. This CD is called the “Server CD” because it contains software for all of the Linux servers. Additional files that may be needed are license and authentication files, and the most recent versions of the software service pack files and G700 firmware files.

The process for upgrading to release 3.0 of Communication Manager varies slightly, depending on the release from which you are upgrading.

Table 12: R3.0 Upgrade requirements depending on pre-upgrade release

Software Release Before Upgrade to Release 3.0	Upgrade Requirement
Release 1.1.x and all other 1.x.x releases not listed below R011x.01.xxx.x	No pre-upgrade service pack required. You need to back up only translation files. Once the hard drive is remastered and the new software is installed on the S8300B, you must reconfigure the media server as if it were a new installation using the Avaya Installation Wizard.
Release 1.2.x, 1.3.0. 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, you can restore all the files using View/Restore Data*.
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, you can restore all the files using View/Restore Data.
Release 2.x R012x.00.0.000.0 R012x.01.x.xxx.x	No pre-upgrade service pack is required. Back up the system and translations files using Backup Now†. Once the hard drive is remastered and the new software is installed on the S8300B, you can restore the files using View/Restore Data.

*. The LMBR backup contains backup sets for the translations, OS and system files.

†. The Data backup contains backup sets for the translations, OS and system files, security files, and AUDIX data, if any

Obtaining service pack files

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.

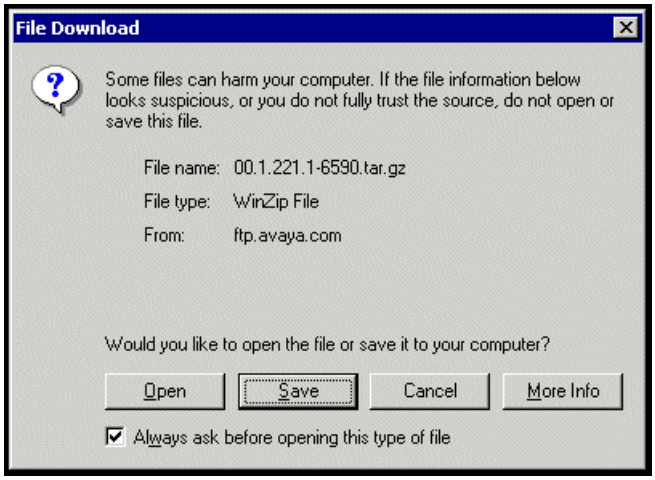
To download a service pack

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, 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 3.0**).
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.

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 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 03.0.526.5-1003.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.

If using IA770, checking stored messages size, obtaining service pack (or RFU) and language files

If IA700 is installed, check the size of stored messages, determine whether an service pack is needed, and/or optional languages are used.

When upgrading Communication Manager to release 3.0 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.

Checking the size of stored messages

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 and documentation can be found on the Avaya Support Web Site at http://support.avaya.com.

To obtain the post-upgrade service pack file and documentation

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.
7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 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, 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 authentication 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 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, S8500, S8700, S8710, or Blade 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.

Preparing for the upgrade on-site

When you arrive on-site, you must perform the following tasks in preparation for the upgrade to release 3.0:

- Accessing the S8300 on page 224
- Checking current software release on page 225
- Pre-Upgrade Tasks — If the S8300 is the primary controller on page 226
- Getting IA770 data and stopping IA770 (if IA770 is being used) on page 230
- Backing up system files on page 233
- Recording configuration information on page 236

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. You will use both Telnet and the Maintenance Web Interface to perform the procedures.

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 48.

To access the S8300 using telnet

1. Click **Start > Run** to open the Run dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.
3. Log in as **craft** or **dadmin**.

   Accept the defaults for Suppress Alarm Origination (`y`) and Terminal Type (`vt100`). At this point, you get the bash prompt and can enter CLI commands.

To access the S8300 using the Maintenance Web Interface

1. Launch the Web browser.
2. 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**.

To access the SAT

1. From the bash CLI, type **SAT** and press **Enter**.

   Or, to open SAT directly from your laptop,

   a. Click **Start > Run**.

   b. Type **telnet 192.11.13.6 5023** and press **Enter**.
2. Log in as *craft* or *dadmin*.
3. Enter **w2ktt** for the **Terminal Type** (if you are running Windows 2000 on your laptop).
4. Accept the default (y) for **Suppress Alarm Origination**.

Checking current software release

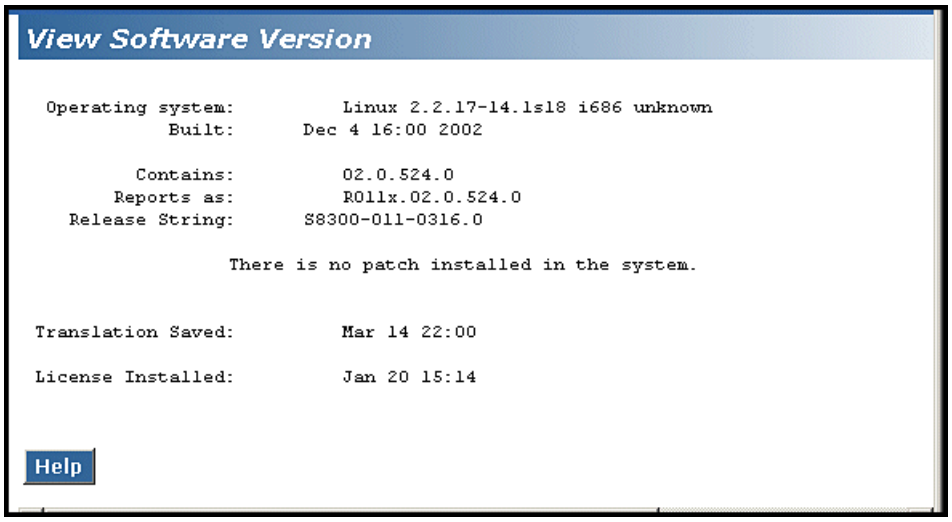
Check the release of Communication Manager currently running on the S8300 to determine whether a pre-upgrade service pack is required.

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 13 maps the release number to the **Reports as:** field, and specifies whether or not a pre-upgrade update is required.

Table 13: 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
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

Pre-Upgrade Tasks — If the S8300 is the primary controller

Skip to Upgrading the S8300A on page 237, 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 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 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 233 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

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.

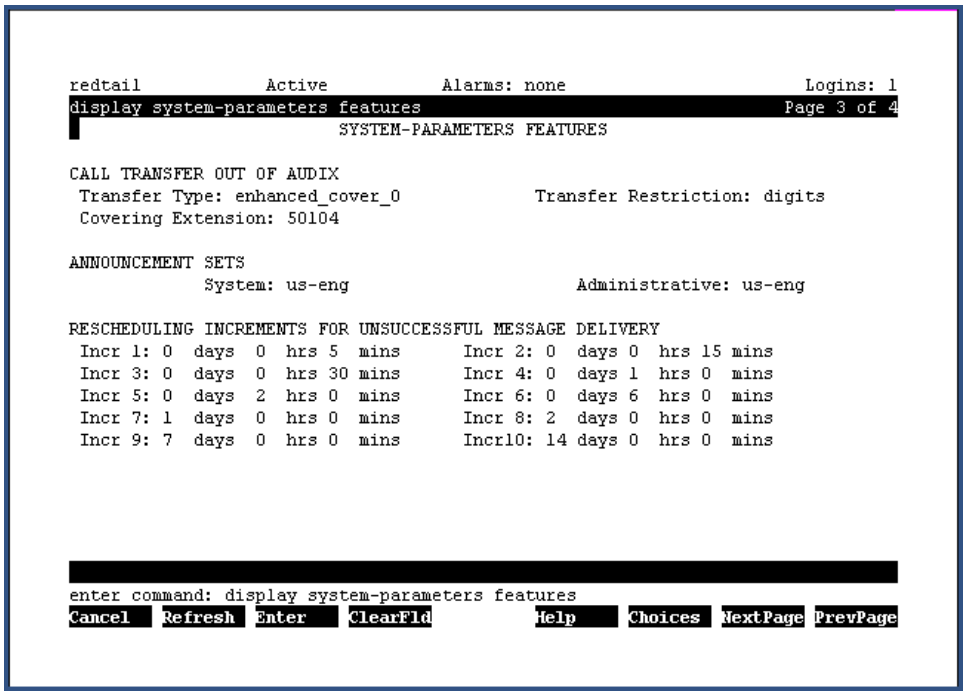
Determining whether optional languages are needed

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



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.

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 3.0 system. If any other language files are listed, you will need to download the additional language files from a language CD after the upgrade.

Stopping 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.

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 1.1.x or 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.

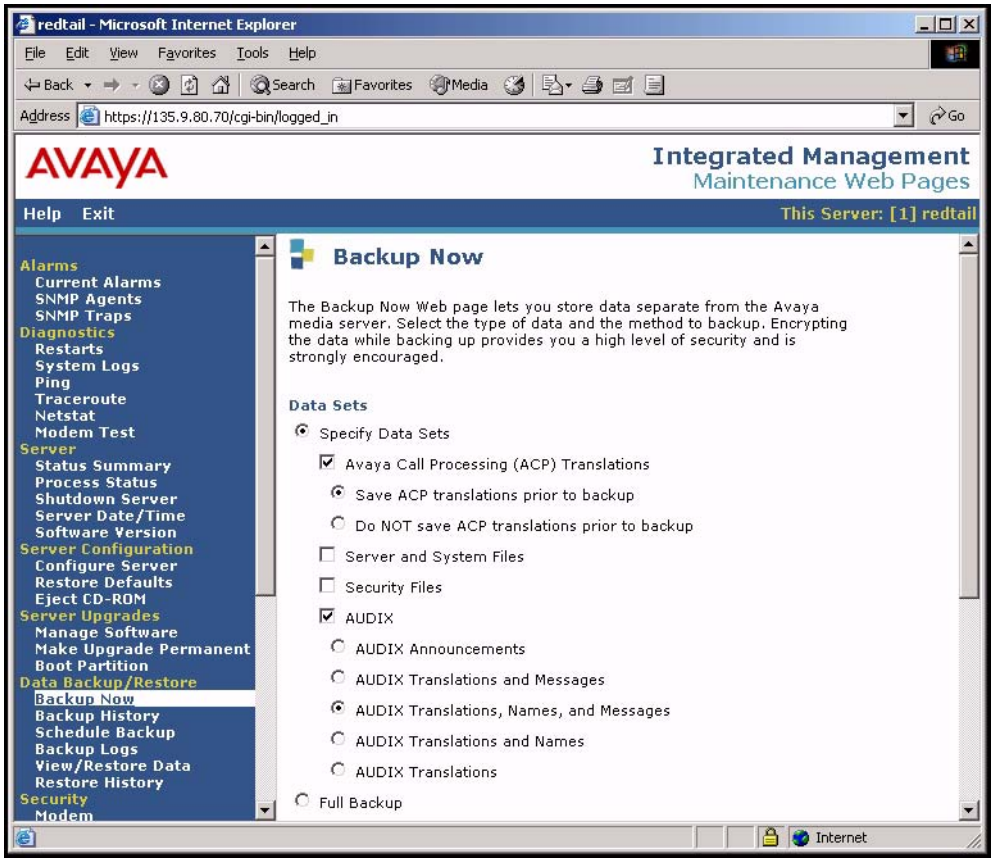
To perform a backup, you need an FTP address, directory path, and a user ID and password to access an FTP server on the customer's network. Check with your project manager or the customer for this information.

To back up data

1. On the Maintenance Web Interface under Data Backup/Restore, click **Backup Now**.

   The **Backup Now** screen displays.

Backup Now screen (Part One)



2. Select all data sets:
   - Avaya Call Processing (ACP) Translations
   - Save ACP translations prior to backup

   Note:

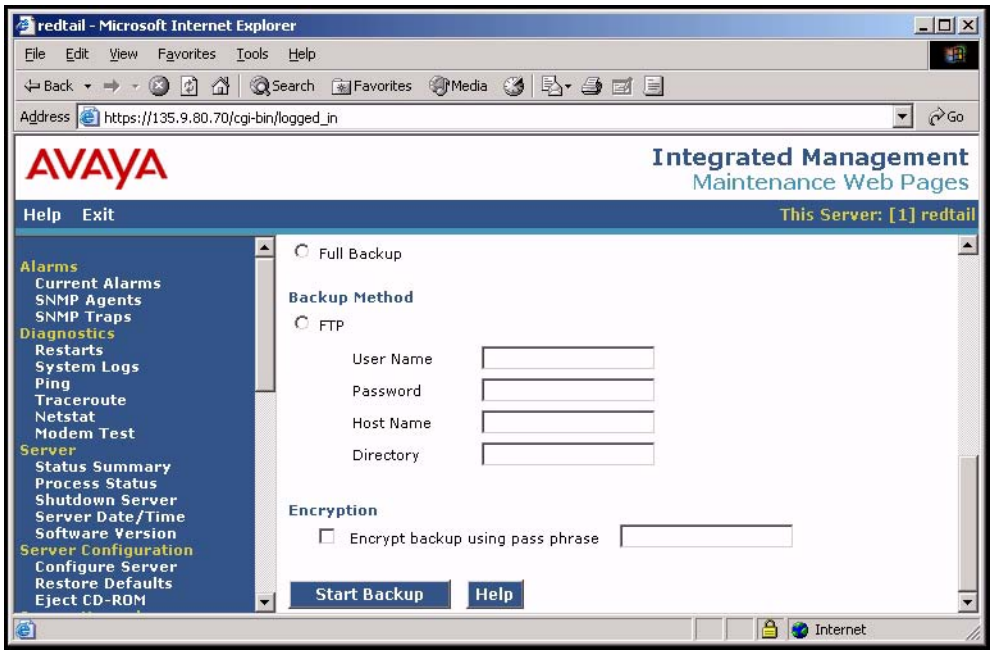
   Select this option only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

   - 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.

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 1.2 or later, most of the configuration data will be re-entered automatically with the restore process. However, if you are upgrading from a pre-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.

7. If upgrading from 1.2 or later, record the data displayed on the **Configure Interface** screen:
   - Server IP address
   - Gateway IP address,
   - Subnet mask

   You can skip the remaining configuration screens.
8. If upgrading from pre-1.2 release, record the data from all configuration screens.

Upgrading 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-3.0 release of Communication manager to release 3.0.

Upgrading an S8300 to release 3.0 requires removing the S8300A and replacing it with an S8300B. The new S8300B should have the remastering program (RP) software installed on its hard drive. The remastering program remasters the hard drive and installs the R 3.0 Communications Manager software. These procedures are described in this section.

This section covers:

- Installing the pre-upgrade software service pack, if necessary on page 238
- Linux migration backup (if current release is 1.2.0 through 1.3.x) on page 240
- Replacing the S8300A with the S8300B Media Server on page 243
- Upgrading Communication Manager software on page 244

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 **1.1.0** and **1.1.9**, or between **2.0.0** and **2.0.9**, skip this service pack installation procedure and go to Replacing the S8300A with the S8300B Media Server on page 243.

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 240.

Note:

Typically, any existing service packs 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 238.

Current release is 2.x, use To install the pre-upgrade service pack when the current release is 2.x. on page 239

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, **03.0.526.5-1003.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, **03.0.526.5-1003**. 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 Manger** 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 Media Server on page 243 if the current software release is 2.x. If you are upgrading from a 2.x release, the Linux Migration Backup may not work. After the upgrade, you will restore data from the system backup you did earlier.

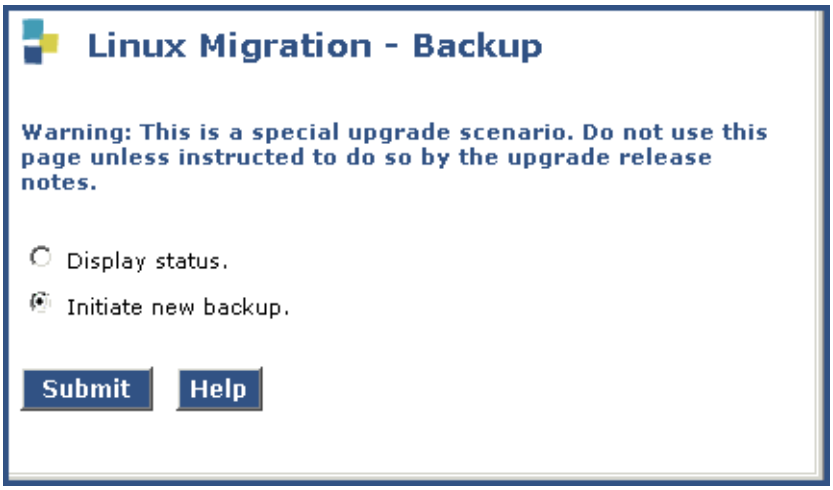
In this section, you will use the Linux Migration Backup procedure on the Maintenance Web Interface to save the system files and translations. After the upgrade, you will use the View/Restore Data feature to restore these files.

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.

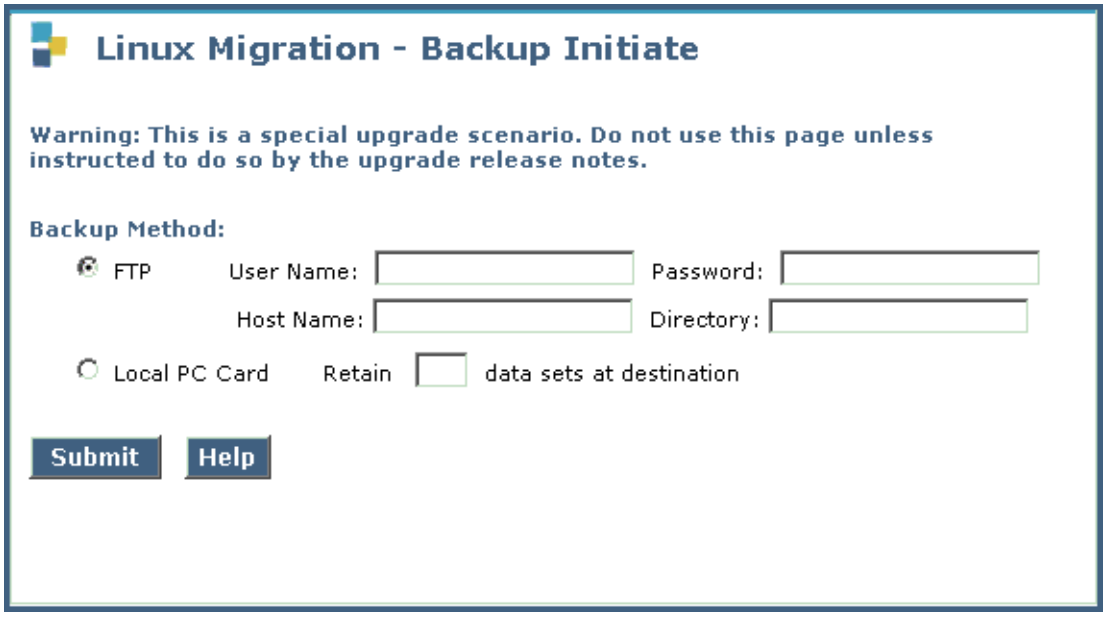
Linux Migration - Backup screen



2. Select "Initiate new backup or restore" and click **Submit**.

   The **Linux Migration - Backup Initiate** screen displays.

Linux Migration - Backup Initiate screen



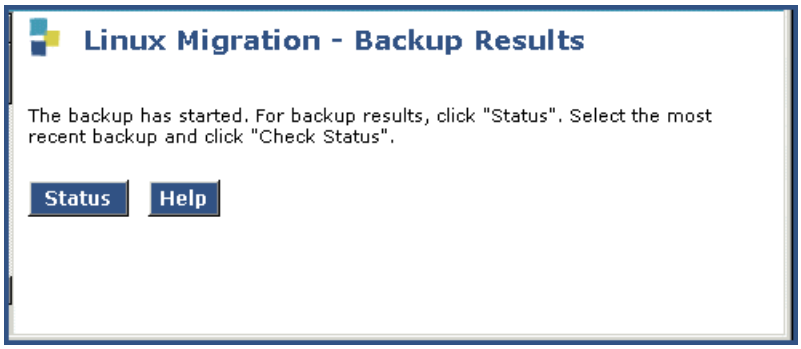
3. Under Backup Method, select FTP

   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

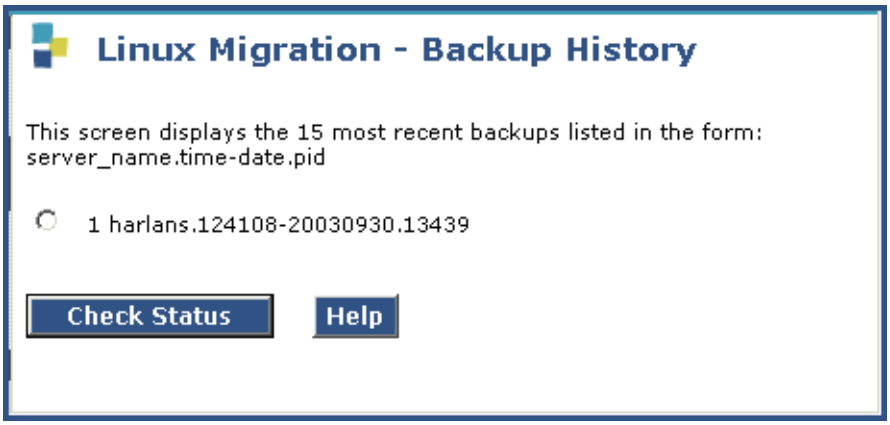


4. Click **Status** to see the backup progress.

   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**.

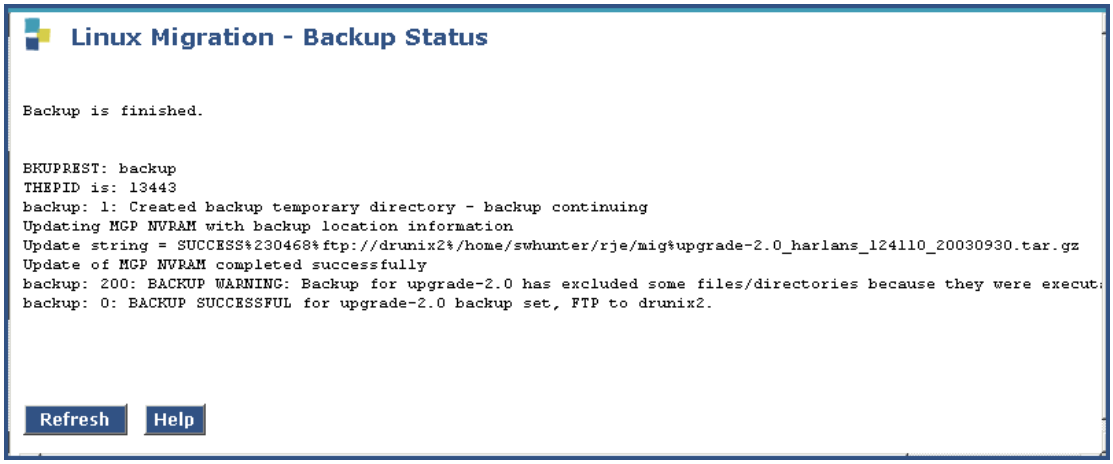
Linux Migration - Backup History screen



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 Media Server

To remove the S8300A and insert the S8300B

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 S8300 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 S8300A, move it from the S8300A to the S8300B.

   Note:

   The CWY1 unit and its associated integration is supported for service packs/ upgrades of existing installations.

8. The LED panel (above slot V1) must be reinserted together with the S8300 circuit pack.

   a. 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.

   b. 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.

9. 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.

10. Reconnect the laptop to the services port of the new S8300B.

Upgrading Communication Manager software

- Setting telnet parameters on page 245
- Remastering the hard drive and installing the upgrade software on page 245
- Verifying software version on page 251
- Copying files to the S8300 on page 252
- Configuring network parameters on page 254
- Verifying connectivity on page 255
- Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) on page 257
- Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x) on page 258
- Verifying the time, date, and time zone on page 262
- Installing post-upgrade Communication Manager service pack file from your laptop on page 256

- Verifying media server configuration on page 262
- Installing the updated license file on page 264
- Installing the new authentication file, if any on page 265
- Saving translations (if not using IA770 and S8300 is not an LSP) on page 266
- Verifying operation on page 266

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 hard drive and installing the upgrade software

To do before you start the upgrade

1. Verify that the S8300B 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.

5. Insert the Server CD in the CD-ROM drive:
   - If TFTP server software is installed on your laptop, ***start the TFTP server program*** (TFTPServer32.exe), and insert the Communication Manager Server CD in the laptop's CD drive.

     CAUTION:

     Verify good AC power connections to the laptop. Do not attempt a remastering using only the laptop's battery power.

   Note:

   Shut down all applications on the laptop except for the TFTP server and the telnet client. Other background applications can overly use laptop resources.

   Note:

   Ensure that the **Outbound file** path is set to the root of your laptop's CD-ROM drive. (For example, D:\)

   To check:

   i. Open the **System** menu in the TFTP server program

   ii. Select **Setup**

   iii. Open the **Outbound** tab.

   iv. To change the **Outbound file** path, click the **Browser** button and select the **CD** drive.

   or,

   - If your laptop does not have TFTP server software installed, attach an external USB CD-ROM drive to one of the USB ports on the S8300B and insert the Server CD in the drive.

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.

NOTE: If you get the login prompt instead of the RP screen

If the telnet login prompt appears instead of the RP screen, the hard drive contains a Communication Manager software release. In this case, if you have a USB CD-ROM drive, connect the drive to a USB port on the S8300 and insert the Server CD. Then log in to the telnet session (using the initial *craft* login) and use the **Shutdown Server** feature on the Maintenance Web Interface to reboot the system. After the reboot completes, telnet to 192.11.13.6 and the RP screen should now be displayed.

If you do not have the USB CD-ROM, you cannot proceed with the upgrade procedure described in this chapter. However, you can upgrade the Communication Manger software using the procedure described in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware and then return to this chapter.

To upgrade using the procedure in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware

1. Complete the procedures starting at Installing the pre-upgrade software service pack on page 658 and ending with Making the upgrade permanent on page 670. Note that you must have a copy of the license and authentication files on your laptop and install them before doing the upgrade.
2. Return to this chapter and complete the procedures starting with Verifying software version on page 251, using the initial *craft* login.
3. Complete all the remaining procedures ***except*** installation of the license and authentication files, which was done in step 1.

Alternatively, you can obtain a USB CD-ROM drive or an S8300B with only the RP software and proceed from Remastering the hard drive and installing the upgrade software on page 245.

The first RP screen

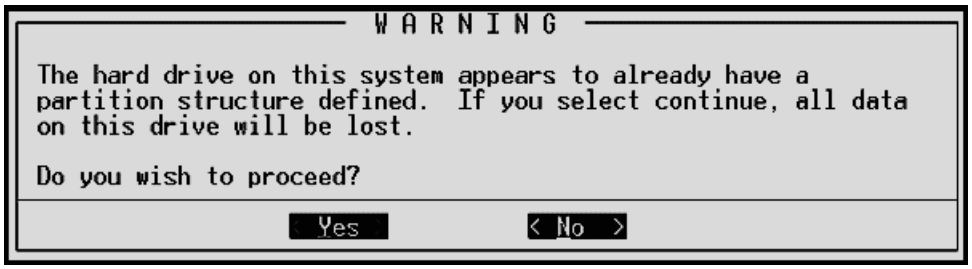
Tip:

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.

4. Select **Install** and press **Enter**.

   If a **Warning** screen appears,

RP Warning screen

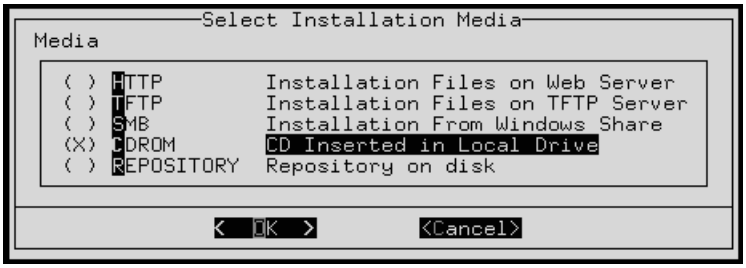


select **Yes** and press **Enter**.

Note:

At this point, the installation script looks for the Server CD either on your laptop or in a CD drive connected to the USB port. If you do not have the TFTP server running on the laptop, and a CD drive is not attached to a USB port, you will see the **Select Installation Media** screen:

The Select Installation Media screen



If you see the Select Installation Media screen:

a. Start up the TFTP server on your laptop, or connect a USB CD-ROM drive to one of the USB ports.

b. Insert the Server CD in the laptop or USB drive.

c. Select either **TFTP** or **CDROM**.

d. Select **OK,** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen

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

6. The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen

7. 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), and select **Yes** at this screen for IA770 installation.

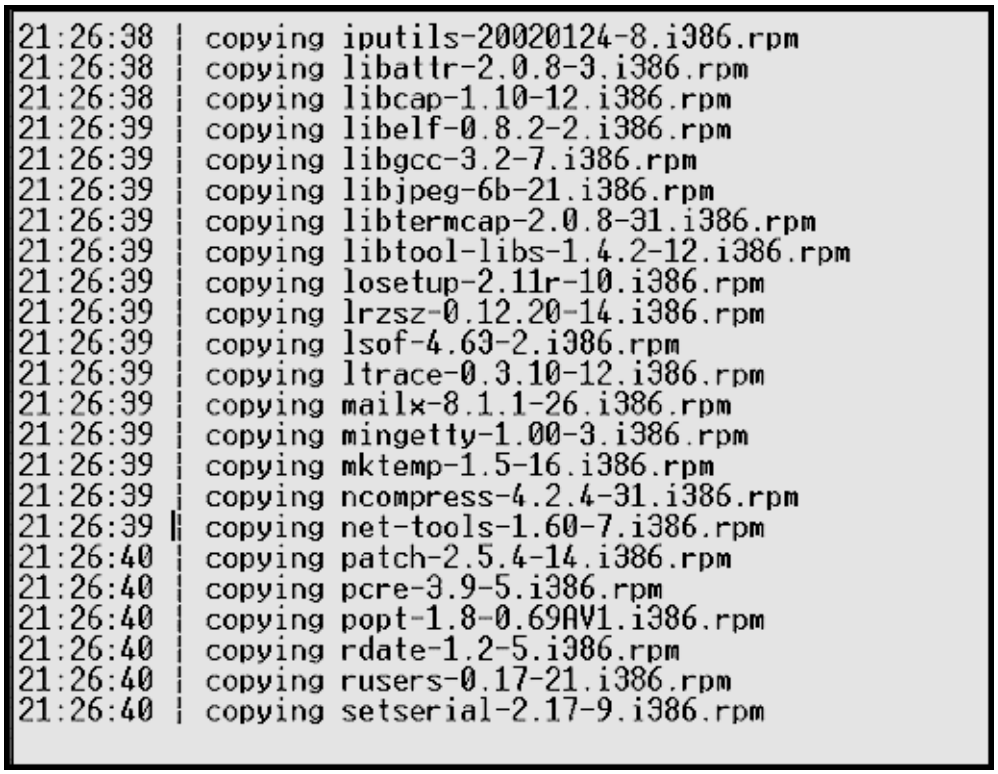
   At this point, the following processes are initiated:

   a. The S8300 hard drive is 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



   These processes take 15–30 minutes.

   d. If IA770 installation has been selected, it is then installed now and enabled.

When the media server is ready to reboot, the following screen flashes for about 5 seconds.

Software and firmware update reminder

When the installation is complete, the CD drive door opens and the system reboots automatically. The reboot takes 1–3 minutes.

In the event you used the laptop TFTP server and you have a problem with power and the S8300 does not reboot, there are two methods of recovery:

- Use the USB CD-ROM to plug into the S8300 and repeat the remastering process using the Server CD.
- Arrange access to another hard drive (comcode 700307028) should it be necessary to perform the TFTP remaster procedure on it.

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 on to Integrated Management and launch the Maintenance Web Interface.
2. Under Server, click **Software Version**.
3. Verify that the media server is running Release 3.0 software.

   The **Report as:** string should show **R013x.01** at the beginning of the string. For example, **R013x.01.0.340.3**.

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

During reformatting of the hard drive, a new directory, /var/home/ftp/**pub**, was created. For release 2.0 and later, this *pub* directory will be used as the /var/home/ftp directory that was used in previous releases.

You must copy the remaining required files to the pub directory on the S8300 hard drive. This includes, but is not limited to:

- the post-upgrade software service pack file
- License file
- Avaya authentication file (if needed)
- New firmware files

To copy files to the S8300

1. Log on to Integrated Management and launch the Maintenance Web Interface.

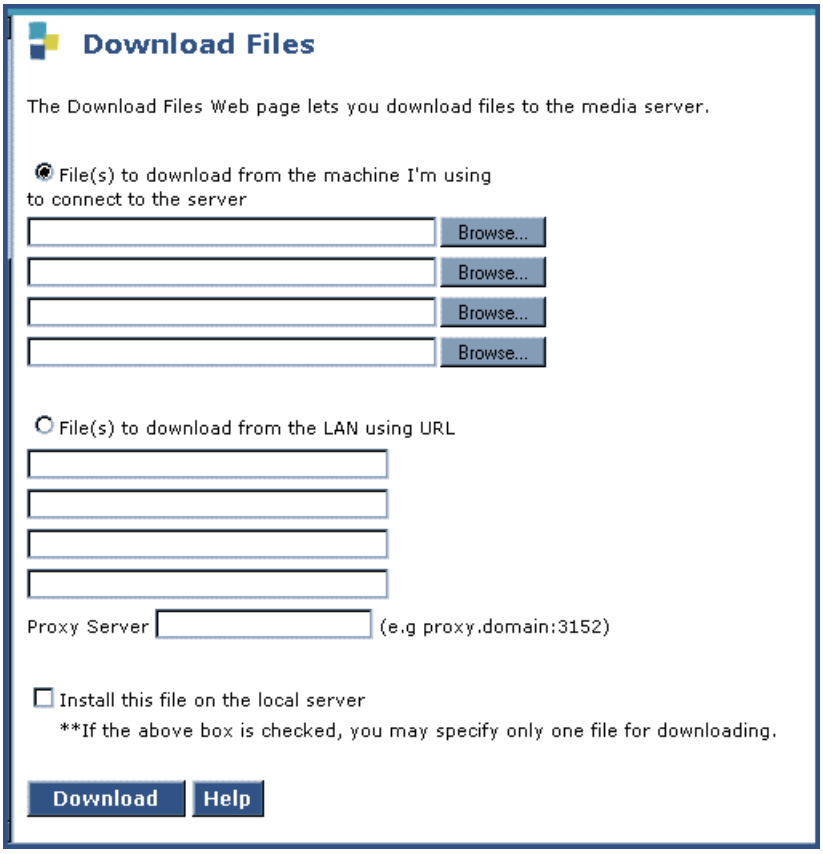
   Note:

   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.)

2. Under Miscellaneous click **Download Files**.

   The **Download Files** screen displays.

Download Files screen



3. 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 are downloading an IP Telephone software file, download this file last with the **Install this file on the local server** checkbox **checked**. Note that the software file must be in a special .tar format to use this feature. See *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507, for information about installing IP Telephone software.

   Note:

   To manually FTP files from your laptop to /var/home/ftp/pub, you must `cd` to pub after starting ftp and logging in; that is, type `cd pub`.

4. 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 Server CD from the CD drive.

Configuring network parameters

Note:

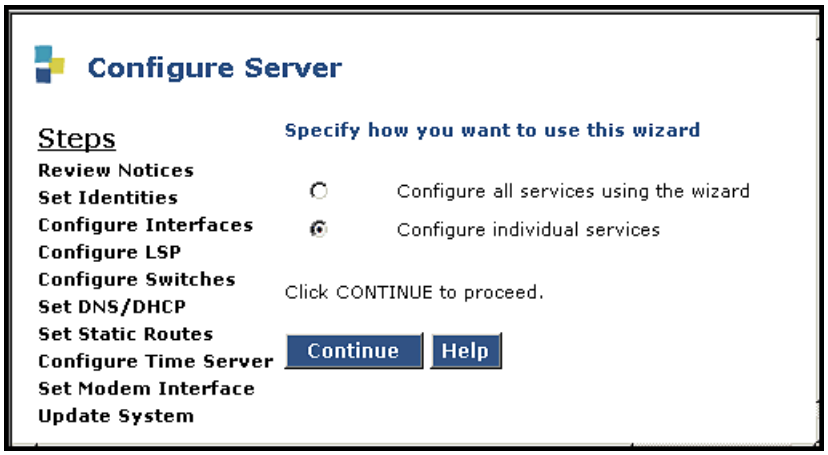
For this procedure, you must have the host name, subnet mask, and IP address of the S8300, and the IP address of the default gateway.

Because the software upgrade resets the configuration data, you must reconfigure the network parameters on the S8300 before restoring the backup files. Also, it is possible that the new software added or changed some of the configuration fields or screens.

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.

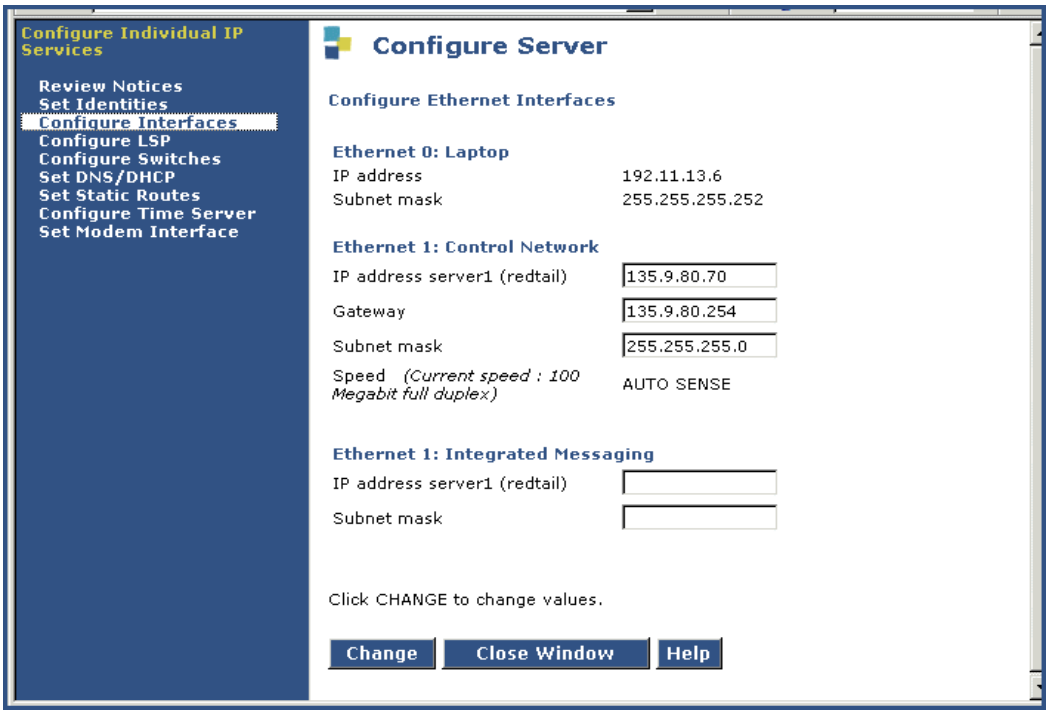
Specify how you want to use this wizard screen



3. Select **Configure individual services** and click **Continue**.
4. Click **Configure Interfaces** from the “Configure Individual IP Services” list on the left.

   The **Configure Ethernet Interfaces** screen displays.

Configure Ethernet Interfaces screen



5. Fill in the correct server IP address, Gateway, and Subnet mask.

   If these fields are already filled in, overwrite them with the correct information. Leave the **Integrated Messaging** fields 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.

6. 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 Linux-Migration backup file is 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.

Installing post-upgrade Communication Manager service pack file from your laptop

CAUTION:

The software service pack may or may not be call-preserving.

Note:

Skip this procedure if there is no Communication Manager service pack file to install.

This service pack may or may not be call preserving.

Use a telnet session to install the service pack file.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **`telnet 192.11.13.6`** and press **Enter**.
3. Log in as **craft**.
4. Type **`cd /var/home/ftp/pub`** and press **Enter** to access the pub directory.
5. At the prompt, type **`ls -ltr`** and press **Enter** to list files in the pub directory.

   The media server displays a list of files in the FTP directory. Verify that the directory contains the Communication Manager .tar.gz file you have uploaded, if any.
6. Type **`update_unpack`** ***`update.tar.gz`***, where ***`update`*** is the release or issue number of the latest software update file. (For example, **`00.0.339.4-xxxx.tar.gz`**). Press **Enter**.
7. Type **`update_show`** and press **Enter** to list Communication Manager files to verify the new software update file was unpacked.
8. Type **`update_activate`** ***`update`***, where ***`update`*** is the release or issue number of the latest software update 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 (reset system 4). 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 software update (patch) was applied.
9. Type **`update_show`** again and press **Enter** to list Communication Manager files to verify the new software update file was activated.

Restoring data

In this section you will restore the system data that you backed up. Do ***only one*** of the following two procedures, depending on how you backed up the data:

- Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) on page 257
- Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x) on page 258

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:

a. On the Maintenance Web Interface, under **Security**, select **Firewall**.
b. In the Service column, find ping.
c. The checkboxes for both **Input to Server** and **Output from Server** should be checked.

Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release)

Do these tasks ***only*** if you have upgraded from a pre-1.2 release.

To restore translations from a pre-1.2 release:

1. Select **View/Restore Data** under **Data Backup/Restore**.
2. Select **FTP** and enter the information for the FTP backup server.

   Click **View**.
3. Select the Communication Manager translations backup set to restore (filename begins with "xln".

   Click **Restore**.

Important:

Do not restore the system or security backup sets (filenames beginning with "os" and "security"). If you backed up the AUDIX data, you will need to restore the AUDIX backup sets as separate steps. The AUDIX translations, names, and messages backup set filename begins with "audix-tr-name-msg". The AUDIX announcement backup set filename begins with "audix-ann".

To configure the server using the Avaya Installation Wizard

If you have upgraded from a pre-1.2 release (Procedure One), you must enter all server configuration information. You can do this most easily using the Avaya Installation Wizard (IW), which will do the server configuration and install the license and password files. If you have filled in the **Electronic Pre-installation Worksheet (EPW)**, the IW will read the configuration data from the EPW. Otherwise, you will need to enter the configuration data into the IW.

In addition, the IW will perform the tasks of upgrading firmware on the G700 Media Gateway and the media modules. When you are finished with the IW, return to Setting rapid spanning tree on the network on page 269.

For information on using the Avaya Installation Wizard, see *Job Aid: Avaya Installation Wizard, 555-245-754.* An interactive demo of the IW can be found at http://support.avaya.com/avayaiw.

Restart the server

You must restart the server to capture the configuration data.

1. Telnet to the S8300 and log on.
2. Type `/opt/ws/drestart 1 4`.

   You will see the response, `Killed`.

Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x)

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:

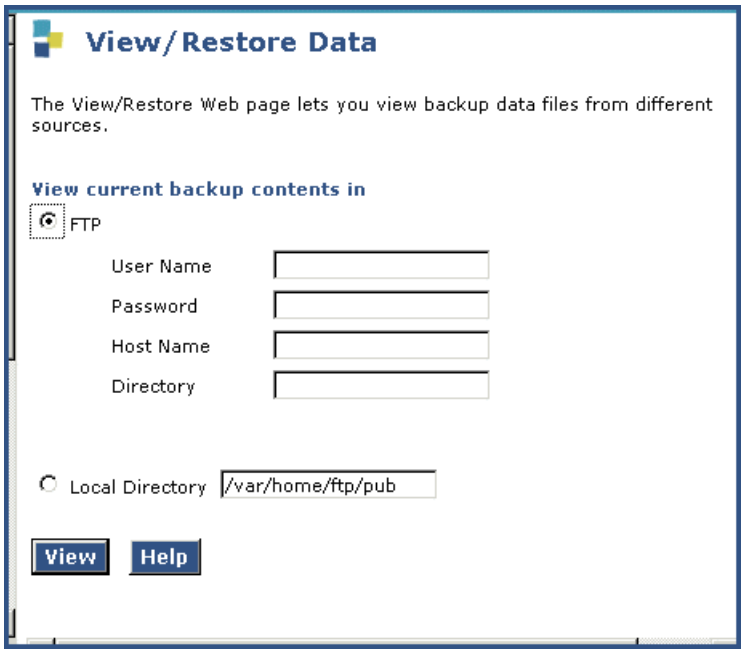
If you used the Linux Migration Backup/Restore backup process, there will be a single backup file with a name starting with "upgrade-2.0." Be sure to restore that backup file, not the backup sets that you may have created with the Data Backup/Restore — Backup Now process. If you restore the wrong files, 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*, 03-300191. After running the remaster command, reboot the S8300 to start the RP program and proceed with Remastering the hard drive and installing the upgrade software on page 245.

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



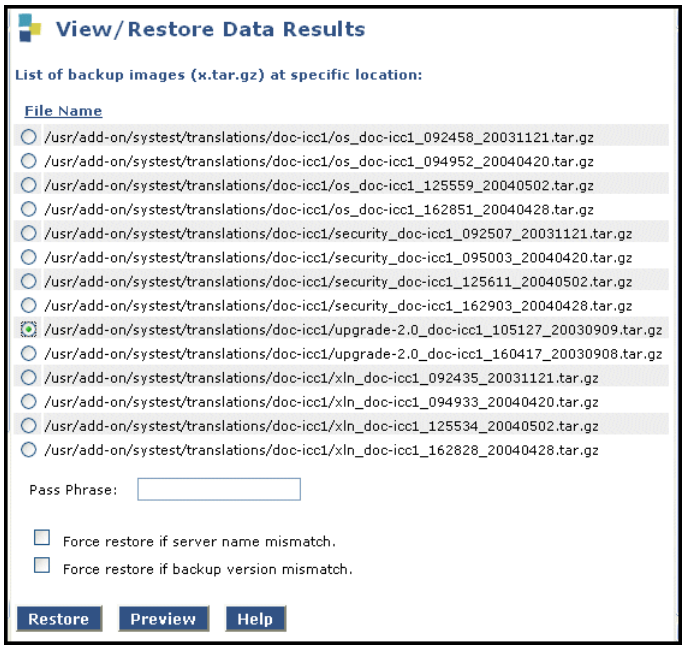
2. Select **FTP**.

   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



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."

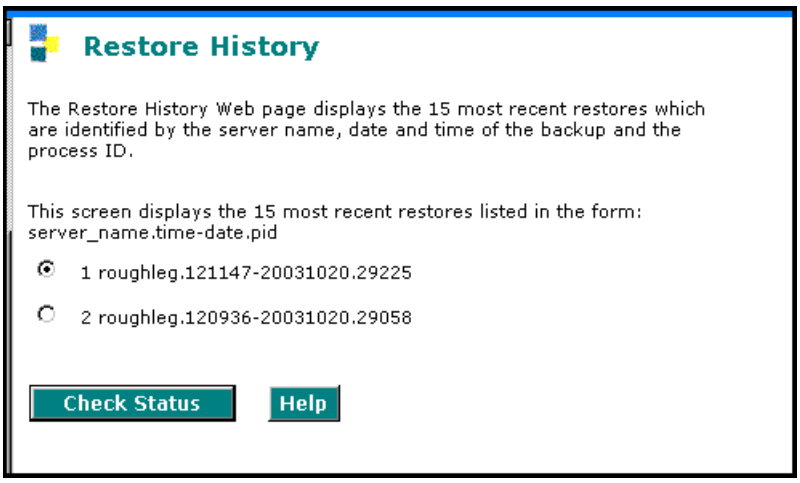
   If you started with a 2.0.x software release and you used the Backup Now procedure, there are three backup files with names starting with "os," "xln," and "security."

   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



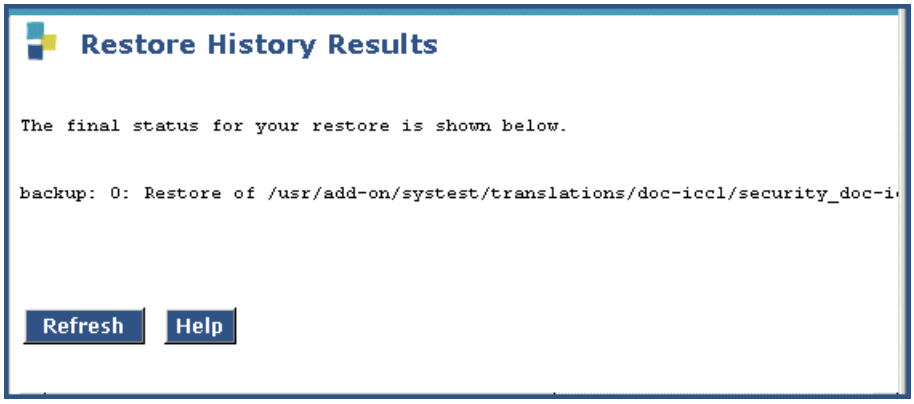
b. Select the backup set being restored and click **Check Status**.

   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



If restoring files from a 2.0.x release, repeat the restore procedure for each backup set, except the AUDIX data (msg and annc files), if any:

- Translations: xln files
- System: os files
- Security: security files

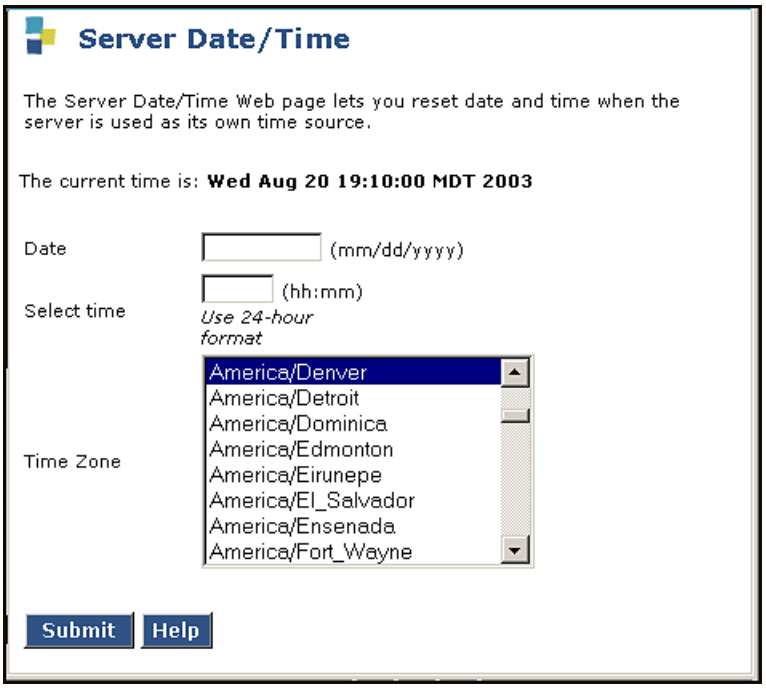
Verifying the time, date, and time zone

To verify the time, date, and time zone

1. Under Server click **Server Date/Time**.

   The **Server Date/Time** screen displays.

Server Date/Time screen



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).

Verifying media server configuration

Note:

If you upgraded from a pre-1.2 release, you should have already completed the server configuration (see To configure the server using the Avaya Installation Wizard on page 258. In this case, skip to Setting rapid spanning tree on the network on page 269.

For the other upgrade scenarios, 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 that the 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. Log on to a Telnet session.
7. Type `/opt/ws/drestart 1 4` to capture the configuration data.

   You will see the response, `Killed`.

Installing the updated license file

CAUTION:

Be sure to install the license file ***before*** the authentication file.

You need to load a new license file when upgrading to a new major release of Communication Manager or when changing the feature set.

Note:

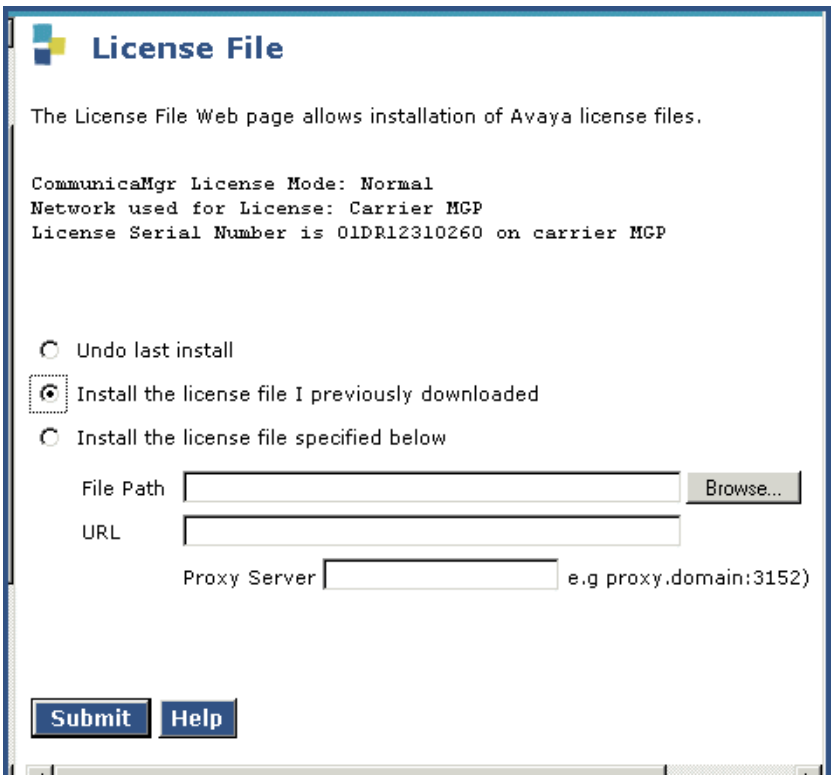
If the S8300 is already set up for remote access, Avaya services personnel can copy new license and authentication files directly into the /pub directory on the server. Avaya personnel will notify you when the new files are in place as agreed (for example, by telephone or E-mail). After they are loaded into the /pub directory, install them using the **License File** and **Authentication File** screens under **Security** on the Maintenance Web Interface.

To install the updated license file

1. On the Maintenance Web Interface under **Security**, click **License File**.

   The **License File** screen displays.

License File screen



2. Select **Install the license file I previously downloaded**.

   Browse to the license file on the services laptop, and click **Submit**. The system tells you when the license is installed successfully.

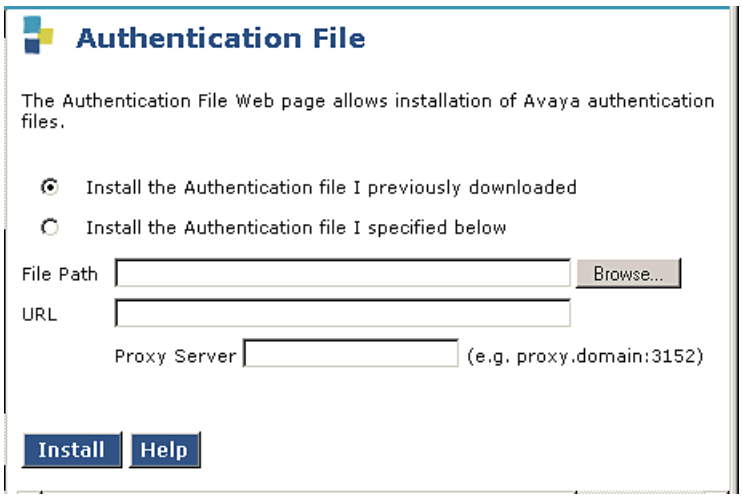
Installing the new authentication file, if any

To install the new authentication file

1. On the Maintenance Web Interface under **Security**, click **Authentication File**.

   The **Authentication File** screen displays.

Authentication File screen



2. Select **Install the Authentication file I previously downloaded**.

   Browse to the authentication file on the services laptop, and click **Install**. The system tells you when the authentication is installed successfully

3. Verify that the restoration of the backup files was successful by testing the *craft* login.

   Telnet to **192.11.13.6** and login as *craft*, using the normal craft password.

   Note:

   If you log into SAT and see the `Translation corruption` message, ignore it for now.

Note:

Avaya Services personnel only: You may need to use the static *craft* password at this point. The 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.

Note:

Avaya Business Partners should call 877-295-0099.

Saving translations (if not using IA770 and S8300 is not an LSP)

Skip this procedure if the S8300 is an ***LSP***, or if ***IA770*** is being used.

CAUTION:

If the system is using IA770, ***do not*** save translations at this time. Skip to Verifying operation on page 266. You will save translations ***after*** installing the new IA770 software.

To save translations (S8300 is not LSP, and IA770 is not used)

1. In a telnet session, open a SAT session.
2. Log in again as *craft*.

   Note:

   If you see the `Translation corruption` message on the first SAT screen, ignore it. Go to Verifying operation on page 266. You will need to save translations later.

3. Type **`save translation`** and press **Enter**.

   When the save is finished, the system displays the message,

   `Command successfully completed.`

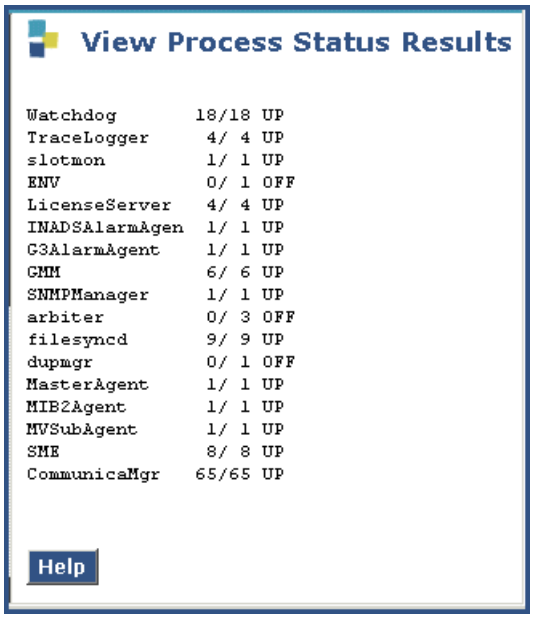
Verifying operation

To verify operation

1. On 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 Results screen



3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**.

   Communication Manager should show **65/65 UP**.

   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.

4. Using a telephone, make test calls to verify that call processing is working.

Next steps

This completes the S8300 upgrade process for upgrading to release 3.0. You now must upgrade the G700 and media module firmware and then restart IA770, if it has been installed on the S8300.

Upgrade the firmware on the G700 Media Gateway

The tasks in this section can be completed most efficiently by using the Avaya Installation Wizard or the Upgrade Tool.

- If the S8300 is a primary controller, use the Installation Wizard.
- If the S8300 is one of several LSPs controlled by the same primary controller, use the Upgrade Tool.

In either case, you can complete the tasks manually by following the procedures in Chapter 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware.

Note:

The IW and Upgrade Tool can also be used to upgrade firmware on the G350.

CAUTION:

If the passwords to log on to the P330 Stack Processor or the media gateway processor (MGP) have been changed from the defaults, you must change them back to the original default passwords before using the Installation Wizard or Upgrade Tool.

Go to http://support.avaya.com/avayaiw to download job aids for using the Installation Wizard or Upgrade Tool.

This section covers:

Upgrading the G700 using the Installation Wizard on page 268

Upgrading the G700 using the Upgrade Tool on page 269

Upgrading the G700 using the Installation Wizard

On the Integrated Management main menu, click **Launch Avaya Installation Wizard**.

To upgrade firmware on the G700 using the Installation Wizard

1. Select the **Upgrade a previously installed Media Server with new software and/or Media Gateway firmware** on the **Usage Options** screen.

   The **Usage Options** screen appears in the Installation Wizard after a few introductory screens.

2. Continue through the Media Server screens, choosing not to upgrade the Communication Manager software.

3. When you get to the **G700 Firmware Upgrade** screen, click the **Action** button to view the versions of the currently installed firmware, and the firmware available in the tftp directory.
4. Select each component for which there is a firmware version that is later than the installed version.

For information on using the Avaya Installation Wizard, see *Job Aid: Avaya Installation Wizard,* 555-245-754. An interactive demo of the IW can be found at http://support.avaya.com/avayaiw.

Upgrading the G700 using the Upgrade Tool

On the Integrated Management main menu, click **Launch Upgrade Tool**. Follow the instructions to upgrade the G700 and media module firmware. For more information on the Upgrade tool, see *Job Aid: Upgrade Tool and Worksheets*, 555-245-757.

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

Complete the following tasks after you have finished the upgrade:

If using IA770:

1. Restore AUDIX data on page 271
2. Saving translations on page 276
3. Installing IA770 service pack (or RFU) files and optional language files, if any on page 276

Complete the upgrade process (S8300 is the primary controller):

4. To check media modules on page 277
5. To enable scheduled maintenance on page 277
6. To busy out trunks on page 277
7. To check for translation corruption on page 277
8. To resolve alarms on page 277
9. To re-enable alarm origination on page 278
10. To back up the system on page 278
11. To restart LSPs (if any) on page 278

If using IA770:

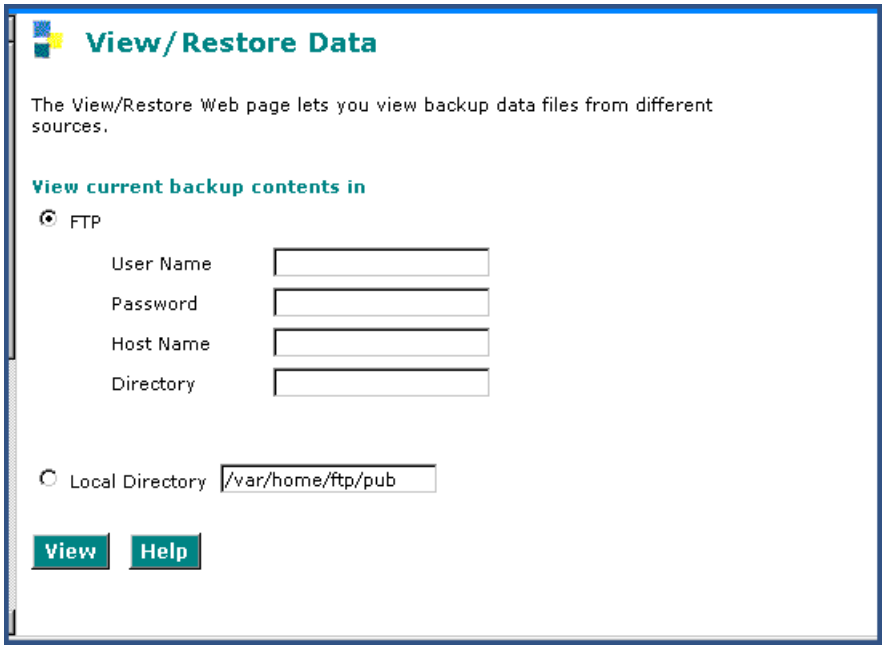
Restore AUDIX data

To restore AUDIX data:

1. Under Data Backup/Restore, click **View/Restore Data**.

   The **View/Restore Data** screen displays.

View/Restore Data screen



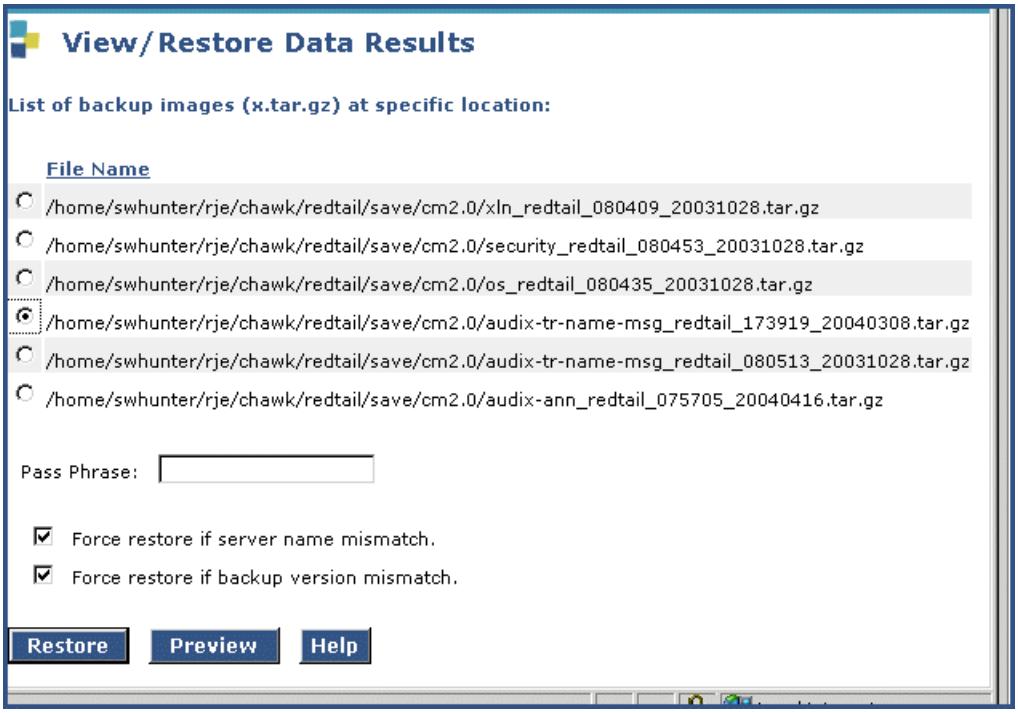
2. Select FTP and enter the information for the location of the backed up **AUDIX Translations**, **Names**, and **Messages** and click **View**.

   The **View/Restore Data Results** screen displays.

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.

View/Restore Data Results screen



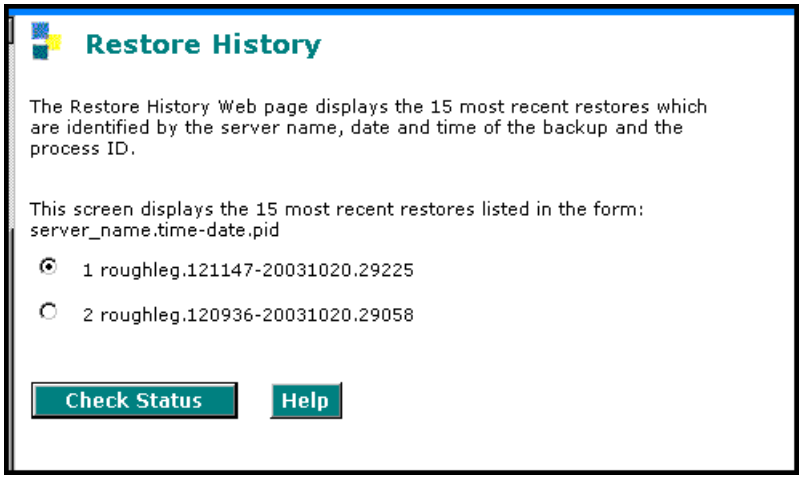
3. Select the **AUDIX Translations, Names, and Messages** backup set (that is, the file with **audix-tr-name-msg** in the filename)
4. Select both **Force** options, and click **Restore**.

To monitor the restore progress:

1. Select **Restore History**.

   The **Restore History** screen displays.

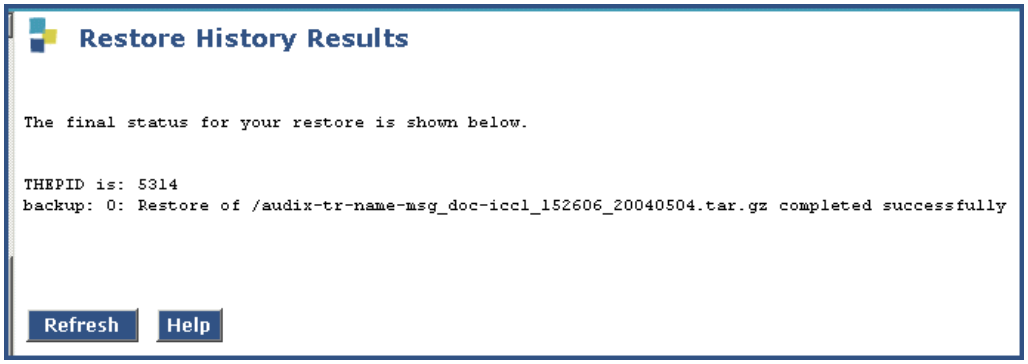
Restore History screen



2. Select the backup set being restored, and click **Check Status**.

   The **Restore History Results** screen displays.

Restore History Results screen



3. Click **Refresh** periodically until the **Completed Successfully** message appears.

   This restore process could take 30 minutes or longer.

   Note:

   Warning messages similar to the message shown on this screen are expected and do not require any action.

To restart Communication Manager and IA770

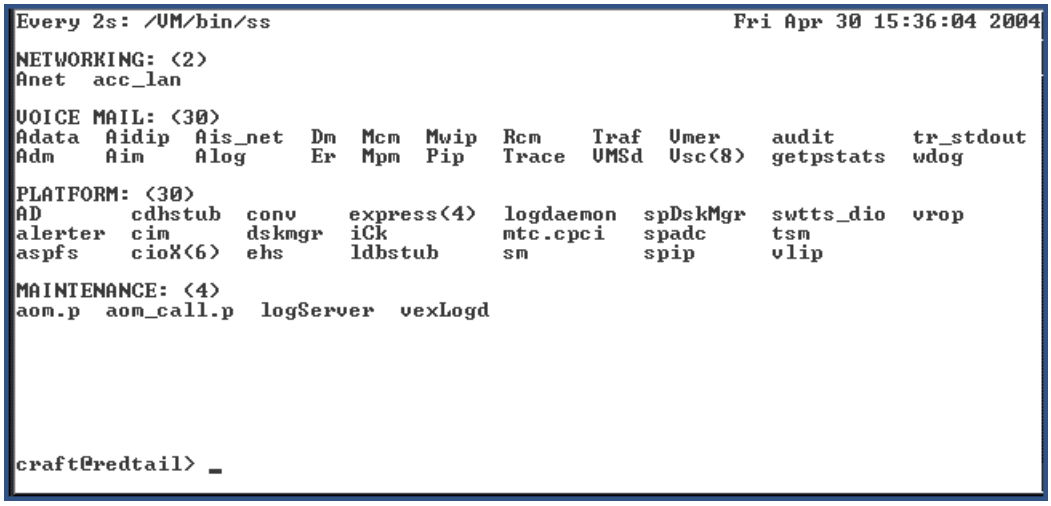
1. Open a Telnet session to the S8300.
2. Type `stop -ac`
3. Type `start -ac`
4. Ensure that all Communication Manager processes come up.

To monitor the startup of IA770:

1. Type **watch /VM/bin/ss**

   The display will periodically refresh automatically. When you see the following display, the IA770 startup is complete.

IA770 startup complete screen



2. Press **Ctrl**+**C** to break out of the **watch** command.

To verify operation:

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

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manger** 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. 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 telnet 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.`

Installing IA770 service pack (or RFU) files and optional language files, if any

If an IA770 post-upgrade service pack is required, you should have downloaded the service pack before coming to the site. If not, you can obtain the service pack from the support Web site at http://support.avaya.com. See the co-located IA770 documentation for procedures to install the service pack.

To install 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.
7. To install the language files, under Miscellaneous click **Messaging Administration**, then **Utilities**, then **Software Management**, then **Software Installation**. Follow the instructions to install the language software.

Complete the upgrade process (S8300 is the primary controller)

Telnet to the S8300 (primary controller) and open a SAT session 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 Pre-Upgrade Tasks — If the S8300 is the primary controller on page 226).

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. Open a Telnet session on the S8300 (LSP).
2. At the command prompt, type **`start -ac`** and press **Enter**.

This completes the upgrade process for a G700 with an S8300.

Chapter 6: Upgrading an existing S8300B to R3.0 using the Wizards

This section covers the procedures to upgrade the software on an installed Avaya S8300B Media Server from a 2.x release to 3.0. This chapter also covers the procedures to upgrade the firmware on an installed Avaya G700 Media Gateway using the Avaya Installation Wizard.

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 5: Upgrading an existing S8300A to R3.0 using the Wizards

About upgrading the S8300B to release 3.0 and upgrading G700 firmware

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 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.
- The Upgrade Tool cannot be used on an S8300 configured as an LSP.

CAUTION:
This upgrade procedure requires a service interruption of approximately 2 hours, or up to 4 hours if IA770 is being used.

In order to upgrade the S8300B to release 3.0, it is necessary to install a pre-upgrade service pack that prepares the server's Web Interface to load the upgrade RPM files from the Server CD onto the S8300 hard drive.

Note:

With release 3.0 of Communication Manager, the Server CD no longer has *.tar or *.tar.gz files. These have been replaced with RPM files that use storage space on the Server CD and the S8300 hard drive more efficiently. To work with these files requires a pre-upgrade service pack installation.

Major tasks to upgrade the S8300B to release 3.0 and upgrade the G700 firmware

The major tasks to upgrade the S8300B to release 3.0, 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:

  - Upgrade the S8300
  - Upgrade the G700 Firmware.
- 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:

- Planning forms provided by the project manager on page 281
- Getting the serial number of the G700, if necessary on page 281
- Checking the number of allocated ports on page 281
- Checking the FTP server for backing up data on page 281
- Obtaining S8300 software and G700 firmware on page 282
- Obtaining service pack files on page 282
- Obtaining service pack and language files, if using IA770 on page 284
- Completing the RFA process (obtaining license and password file) on page 285

Planning forms provided by the project manager

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, passwords, people to contact, the type of system, and 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.

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 3.0), you will need the serial number of the G700. To get this number, ask the customer's administrator to log in to 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

Release 3.0 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. Ask the customer to check the system for the maximum number of ports. This can be done using the SAT command, **`display system-parameters customer-options`**. Verify that the **Maximum Ports:** field is `900` or less.

Checking the FTP server for backing up data

During the installation and upgrade procedures, you will need to back up the system data to an FTP server. Normally, you will use an FTP server on the customer's LAN for backups.

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

Check with your project manager or the customer for this information.

Important:
Before going to the customer site, make sure that you can use a customer server 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 a CD-ROM that you take to the site. This CD is called the “Server 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)

Note:
The necessary changes in the Web Interface and script/command changes are available in a required pre-upgrade update to be used for the upgrade from releases 2.x to release 3.0.

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

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 14: 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 3.0. You must escalate.

Table 14: 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.02.0.xxx.x	02.0.xxx.x-xxxx.tar.gz

To download service packs to the laptop

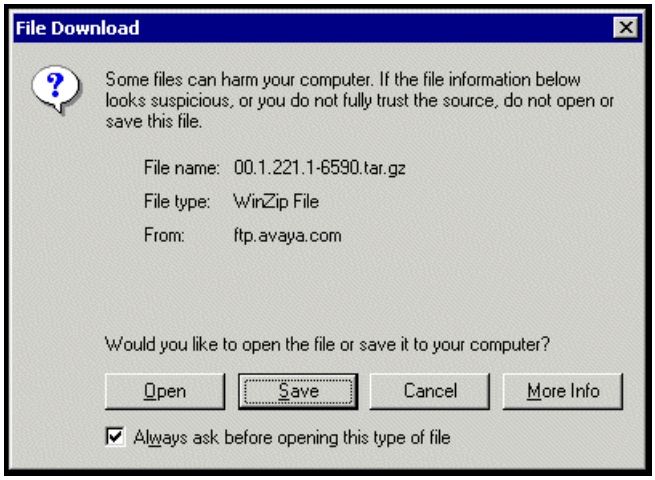
1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access http://www.avaya.com/support on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At the Avaya support site, 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 3.0**).
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, if using IA770

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 3.0 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 **Messaging** in the list on the left.
2. Scroll down to the INTUITY links and double click on **IA 770 INTUITY AUDIX Messaging Application**.
3. Double click on **All Documents**.
4. Under Software Download, double click on the service pack for this release. For example, **IA 770 INTUITY AUDIX Embedded Messaging Application Patches for 3.0**.
5. Double click on the file name. For example, **C6039rf+c.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 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, S8500, S8700, S8710, or Blade 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.

On-site Preparation for the Upgrade

Perform the following tasks before starting the software upgrade on the S8300:

- Accessing the S8300 on page 288
- Completing pre-upgrade tasks — If the target S8300 is the primary controller on page 289
- Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used) on page 292
- Backing up S8300 recovery system files on page 296
- Copying license and authentication files to the S8300 hard drive (from your laptop) on page 300
- Saving translations (only if new license and/or authentication files installed) on page 313
- Copying the software and firmware files from the Server CD on page 302

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 48.

You will use both telnet and the Maintenance Web Interface to perform the procedures.

To access the S8300 using telnet

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.
3. Log in as *craft* or *dadmin*.

To access the S8300 using the Maintenance Web interface

1. Launch the Web browser.
2. 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**.

To access SAT

1. From the bash CLI, type **SAT** and press **Enter**.

   Or, to open SAT directly from your laptop,

   Click **Start > Run**, type **telnet 192.11.13.6 5023**, and press **Enter**.
2. Log in as *craft* or *dadmin*.
3. Enter **w2ktt** for the **Terminal Type** (if you are running Windows 2000 on your laptop).
4. Accept the default (`y`) for **Suppress Alarm Origination**.

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 307.

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 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 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 (AUDIX) Data and Stopping IA770 (if IA770 is being used)

Skip to Backing up S8300 recovery system files on page 296 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

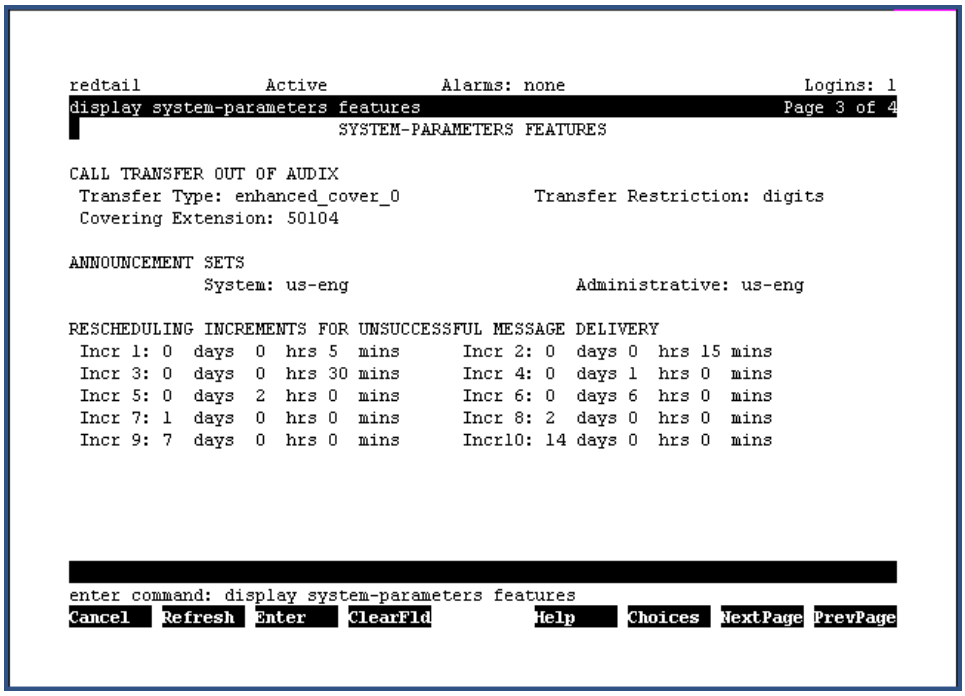
To determine the system language

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



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 Manger 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 295 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

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.

Backing up S8300 recovery system files

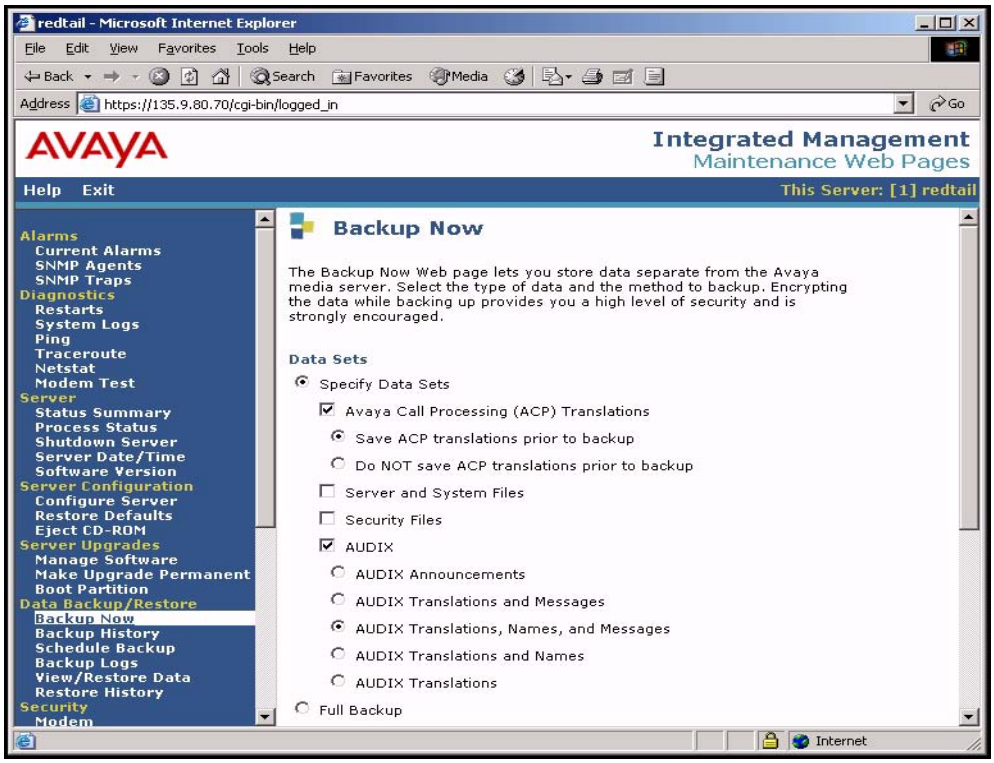
Before installing the S8300 software, back up the system data in case you need to back out of the upgrade. You should back up to an FTP server on the customer's network. To do this, you need an FTP address and directory path and a user ID and password to access the customer's network. Check with your 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 all data sets:
   - Avaya Call Processing (ACP) Translations
   - Save ACP translations prior to backup

   Note:

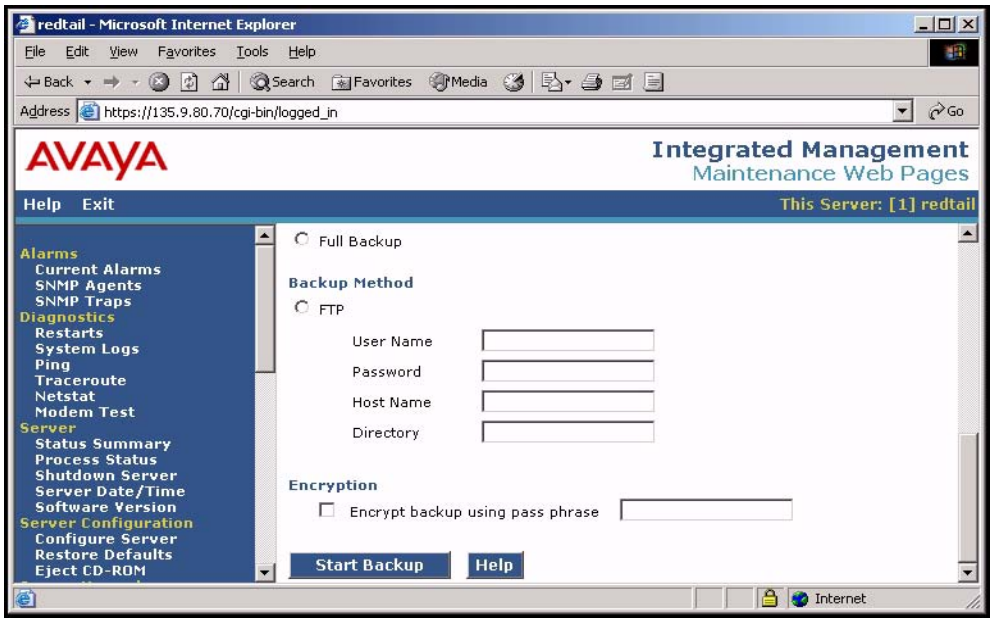
   Select this option only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

   - 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.

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

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

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 3.0 to complete successfully.

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 license and authentication files to the S8300 hard drive (from your laptop)

Skip to Copying the software and firmware files from the Server CD on page 302 if you are not installing a new license or password file.

For an upgrade, you need to install a license file when:

- Upgrading to a new major release of Communication Manager (for example, R2.x to R3.0)
- Changing the feature set

Note:

If the S8300 is already set up for remote access, Avaya services personnel can copy new license and authentication files directly into the FTP directory on the server. Avaya personnel will notify you when the new files are in place as agreed (for example, by telephone or E-mail). After they are loaded into the FTP directory, install them using the **License File** and **Authentication File** screens from the S8300 main menu web-page.

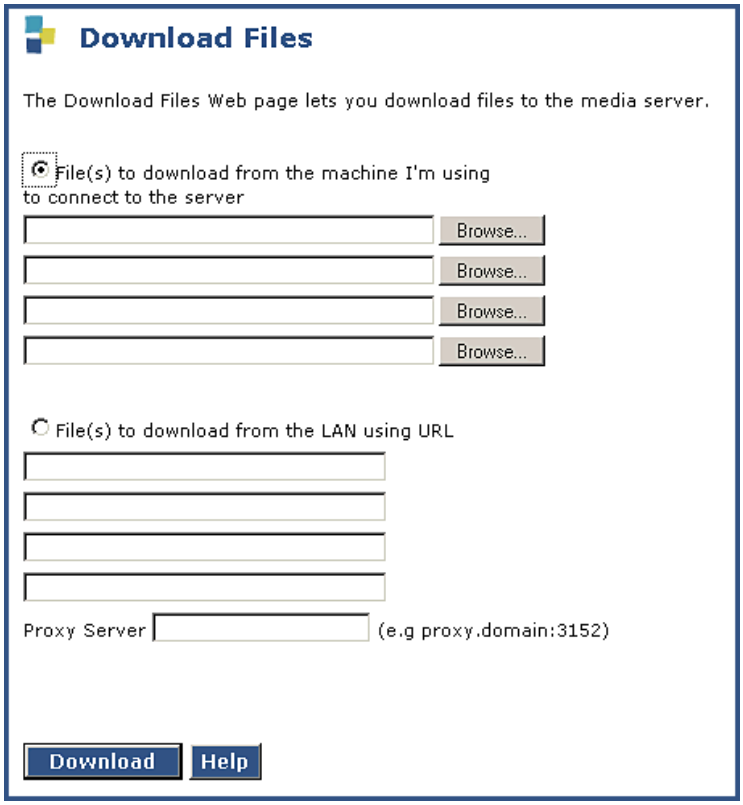
Use the following procedure to transfer the license and password files from the CD or hard drive on your laptop to the S8300 hard drive.

To copy license and authentication files to the S8300 hard drive from your laptop

1. Log on to the S8300 Web Interface
2. In the main menu under Miscellaneous, click **Download Files**.

   The **Download Files** screen displays.

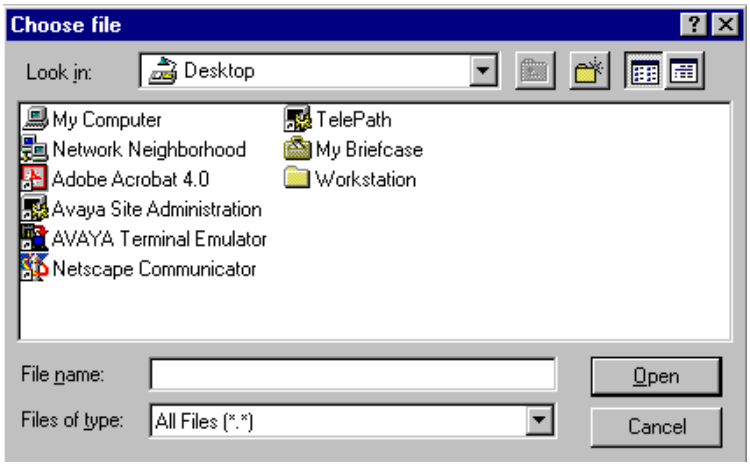
Download Files screen



3. Select **Files to download from the machine I'm using to connect to the server** and click **`Browse`** for the first field.

   The S8300 displays the **Choose File** screen, which allows you to select files from your laptop.

Choose File Screen



4. Locate the customer's license (**.lic**) file.
5. When you have selected the **.lic** file, click **Open** in the dialog box.
6. Click **Browse** for the second field.
7. Locate the customer's **.pwd** file on your laptop.
8. When you have selected the **.pwd** file, click **Open** in the dialog box.
9. When you have finished entering the files to be copied, click **Download**.

   When the files are successfully transferred, the system displays the status screen.

Copying the software and firmware files from the Server CD

Normally, during an upgrade, you will have the Server 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*, 012-01.0.411.1). The latest service pack software for Communication Manager also reflects the most recent load of software (*for example only*, 01.0.411.1-6592).

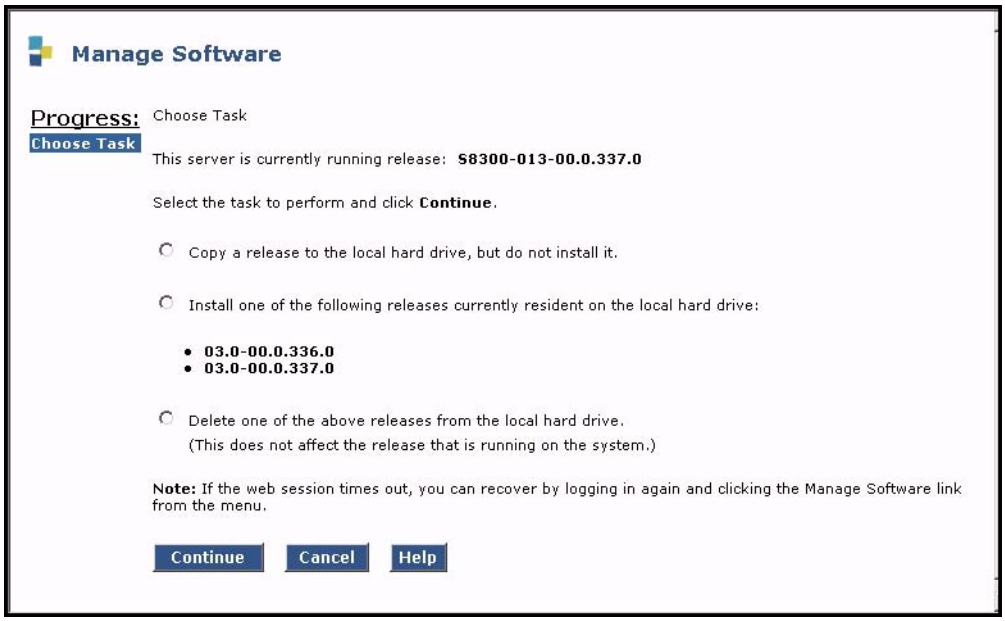
These files also contain the most recent firmware for the G700 Media Gateway, the various media modules, and the P330 Stack Processor.

To transfer files from the Server CD

1. Insert the Server CD into the CD-ROM drive.
2. Log in to the S8300 Web interface.
3. Under Server Upgrades, click **Manage Software**.

   The **Manage Software** screen displays.

Manage Software screen



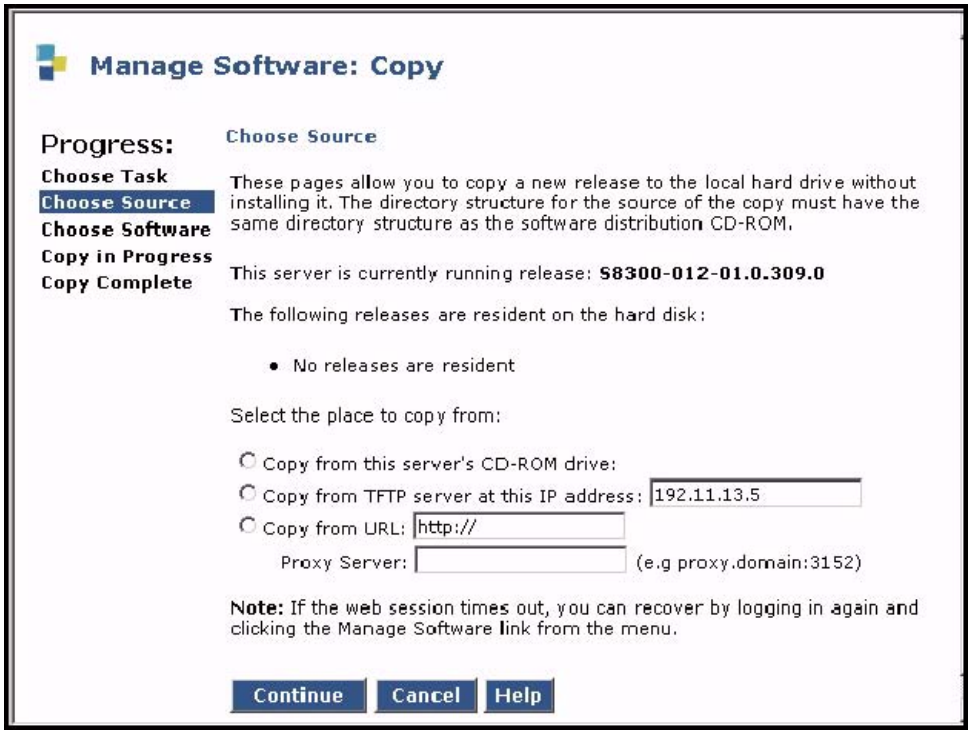
4. Select the radio button **Copy a release to the local hard drive, but do not install it**.

   Note:

   The S8300 hard drive can hold up to three releases without having to delete a release before copying a new release from the Server 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



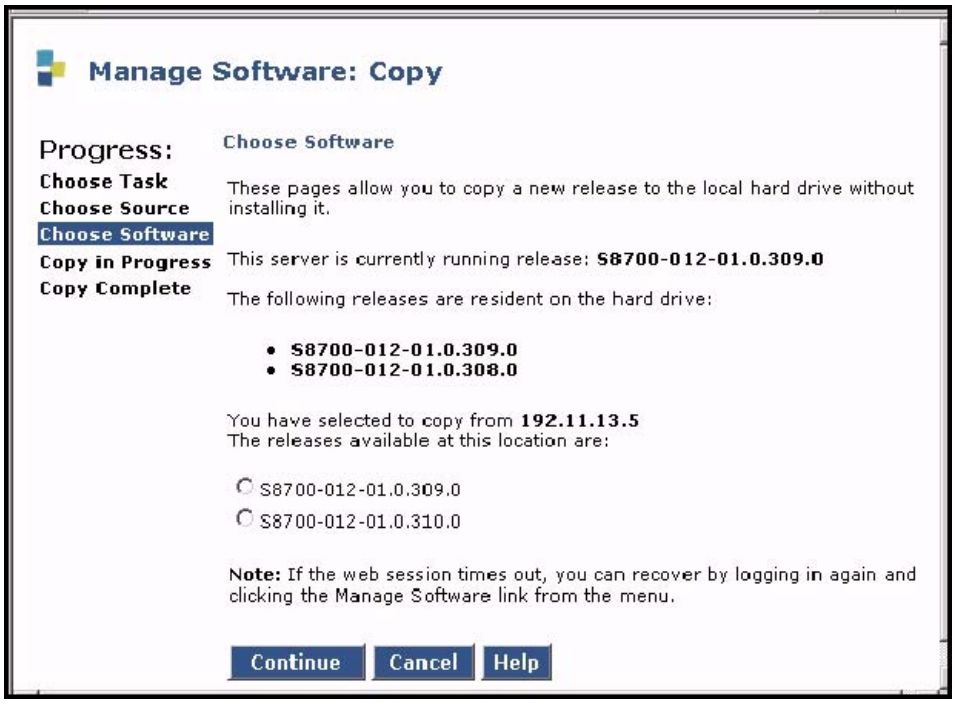
Possible sources include:

- 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.

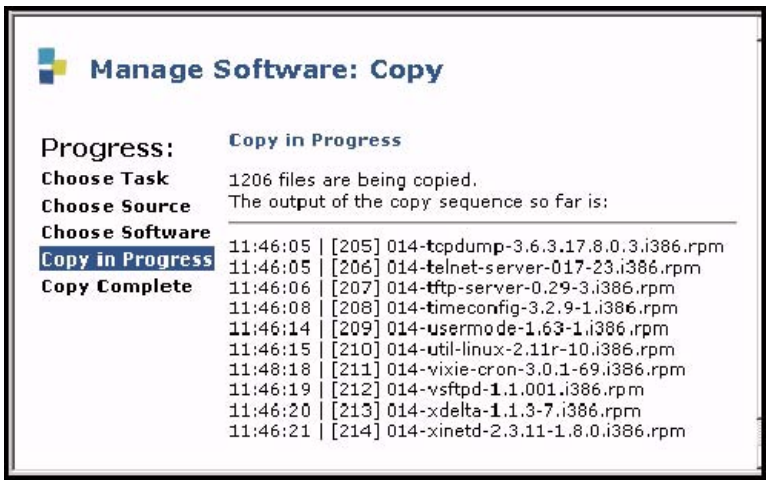
The **Choose Release** screen displays.

Choose Release screen



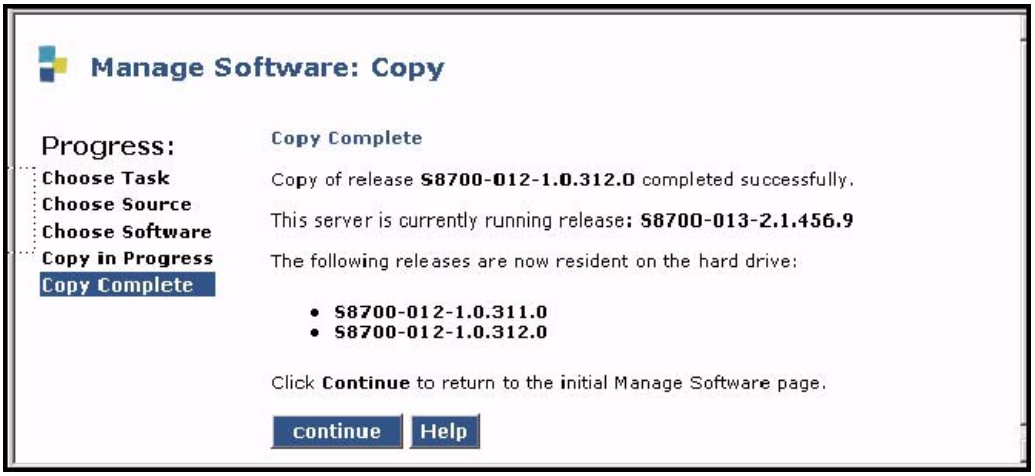
The screen is presented with no radio button selected. The user must select the release to be copied and click **Continue**. The **Copy in Progress** screen displays.

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.

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 S8300 Media Server to Communication Manager release 3.0.

Upgrading the S8300B using the Web Interface

Perform the following tasks to upgrade the S8300 to the most recent load of software:

1. Installing new software on page 307
2. Making the upgrade permanent on page 311
3. Installing post-upgrade Communication Manager service pack, if any on page 311.

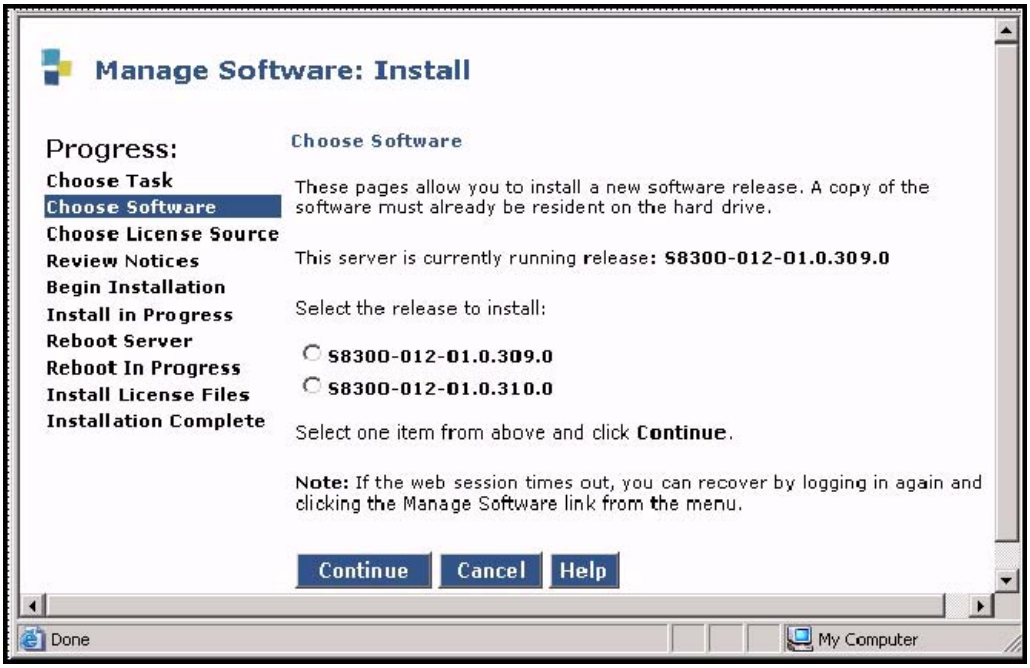
Note:

You can also use the Upgrade Tool to perform these tasks.

Installing new software

The first step in upgrading the S8300B Media Server to Communication Manager 3.0 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 from the Server CD on page 302). 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.

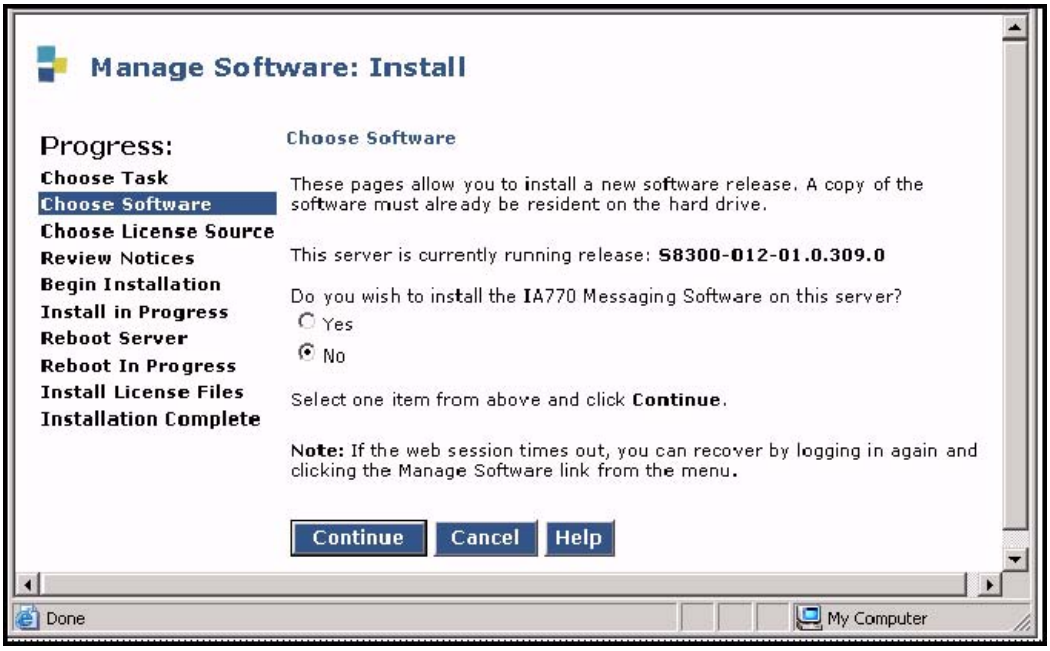
Choose Software screen



This screen will show the release currently running on the S8300B, and the releases resident on the hard drive. To install the 3.0 release, click the radio button next to the 3.0 release and click **Continue**.

The next screen displays in order to support installation of IA770 software.

IA770 Installation Support screen



This screen displays, if and only if:

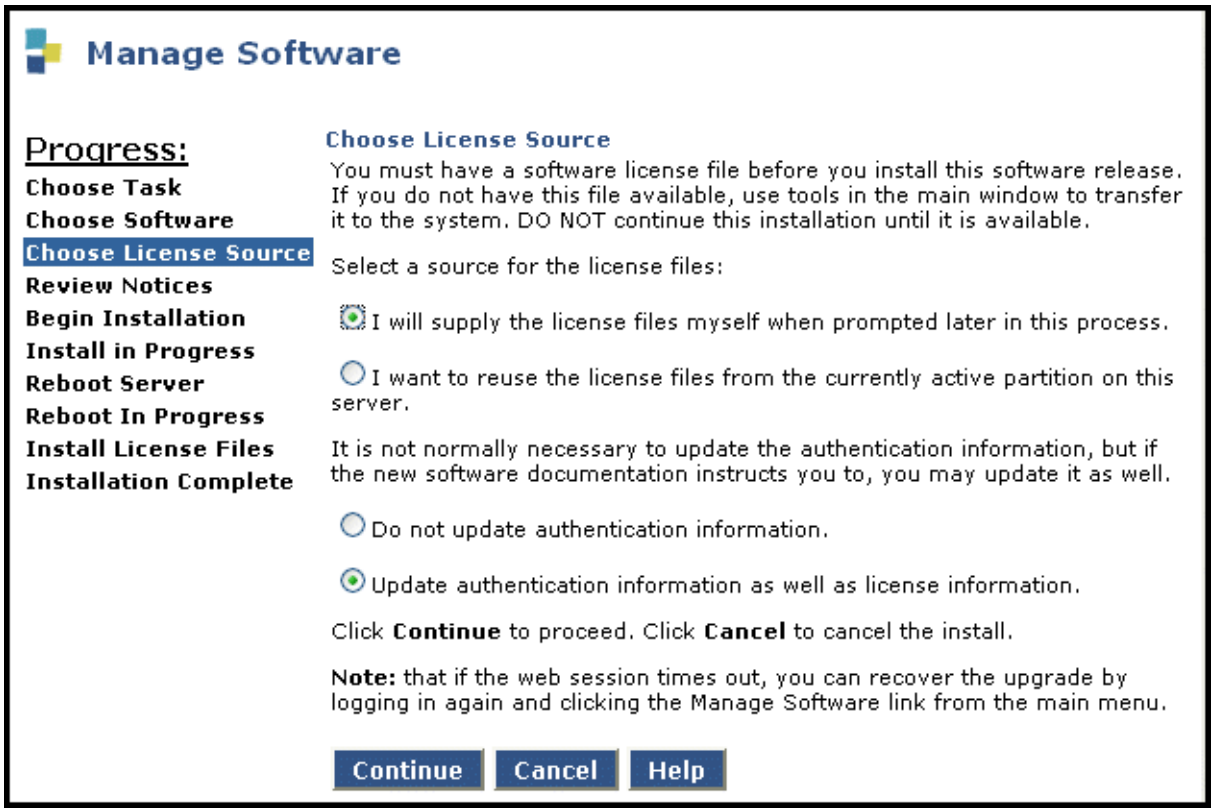
- IA770 is/is not supported, and
- The server is not an LSP.

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.



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.

   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.

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.

12. Under Server, click **Software Version** to verify the new software version.

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

Installing post-upgrade Communication Manager service pack, if any

Note:

Skip this procedure if there is no Communication Manager service pack file to install.

This service pack may or may not be call preserving.

Use a telnet session to install the service pack file.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.
3. Log in as **craft**.
4. Type `cd /var/home/ftp/pub` and press **Enter** to access the pub directory.
5. At the prompt, type `ls -ltr` and press **Enter** to list files in the pub directory.

   The media server displays a list of files in the FTP directory. Verify that the directory contains the Communication Manager .tar.gz file you have uploaded, if any.

6. Type `update_unpack` ***`update.tar.gz`***, where ***`update`*** is the release or issue number of the latest software update file. (For example, `00.0.339.4-xxxx.tar.gz`). Press **Enter**.
7. Type `update_show` and press **Enter** to list Communication Manager files to verify the new software update file was unpacked.

8. Type **update_activate *update***, where ***update*** is the release or issue number of the latest software update 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 (reset system 4). 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 software update (patch) was applied.

9. Type **update_show** again and press **Enter** to list Communication Manager files to verify the new software update file was activated.

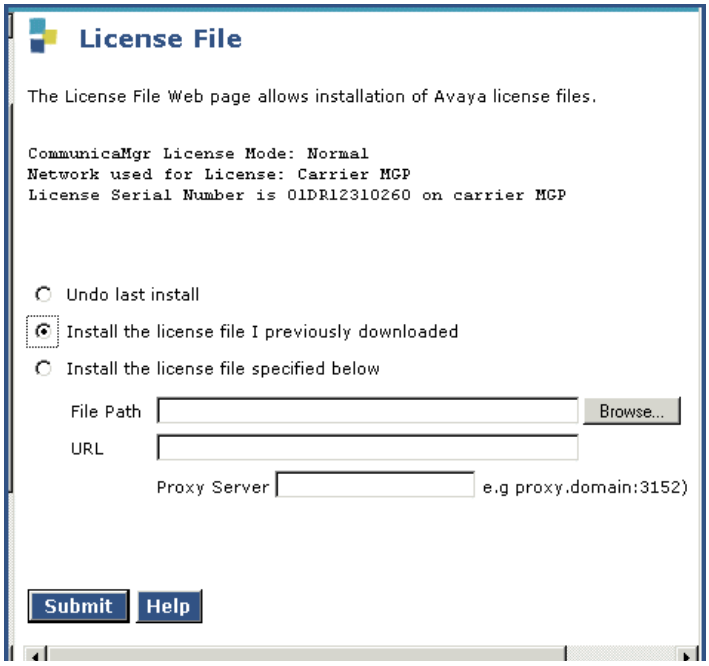
Install updated license and authentication files

To install the license and authentication files:

1. On the Maintenance Web Interface menu under Security, select **License File**.

   The system displays the **License File** screen.

License File Screen

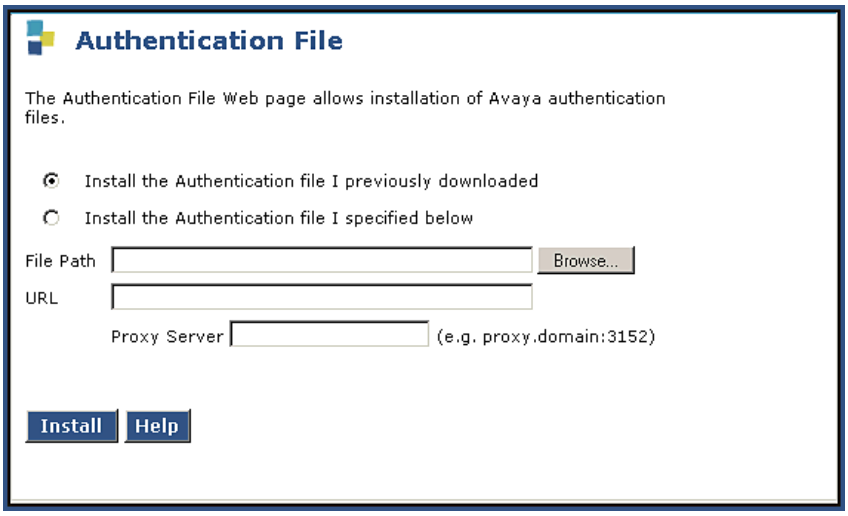


2. Select **Install the license file I previously downloaded** and click **Submit**.

   The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.
4. The **Authentication File** screen displays.

Authentication File screen



5. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system tells you the authentication file is installed successfully

Saving translations (only if new license and/or authentication files installed)

Skip this procedure if the S8300 is an LSP.

To save translations

1. In the telnet session, open a SAT session. and log in as *craft* (or *dadmin*).
2. At the SAT prompt, type **`save translation`** and press **Enter**.

   When the save is finished, the system displays the message,

   `Command successfully completed.`

Upgrade the G700 Firmware

This section describes upgrading firmware on the components of the G700, including the Media Gateway Processor (MGP), the P330 Stack Processor, and any installed media modules.

The tasks in this section can be completed most efficiently by using the Avaya Installation Wizard (IW) or the Upgrade Tool. If the S8300 is a primary controller, use the Installation Wizard. If the S8300 is an LSP, use the Upgrade Tool on the primary controller. Or, in either case, you can complete the tasks manually as described in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware.

Choose one of the upgrade options:

- Upgrading G700 firmware using the installation wizard on page 314
- Upgrading G700 firmware using the upgrade tool from the primary controller on page 318

Note:

The IW and Upgrade Tool can also be used to upgrade firmware on the G350.

Go to http://support.avaya.com/avayaiw to download job aids for using the Installation Wizard or Upgrade Tool.

Upgrading G700 firmware using the installation wizard

Important:

The IW, running on an S8300 primary controller in a stack, can be used to upgrade G700 firmware on any G700 in the stack; that is, G700s connected by the Octaplane cable. However, the IW cannot be used to upgrade G700s connected to the primary controller over the LAN and not connected in the stack.

CAUTION:

If the passwords to log on to the P300 stack or the MGP have been changed from the defaults, you must change them back to the original default passwords before using the Installation Wizard or Upgrade Tool. The IW will prompt for new passwords.

Important:

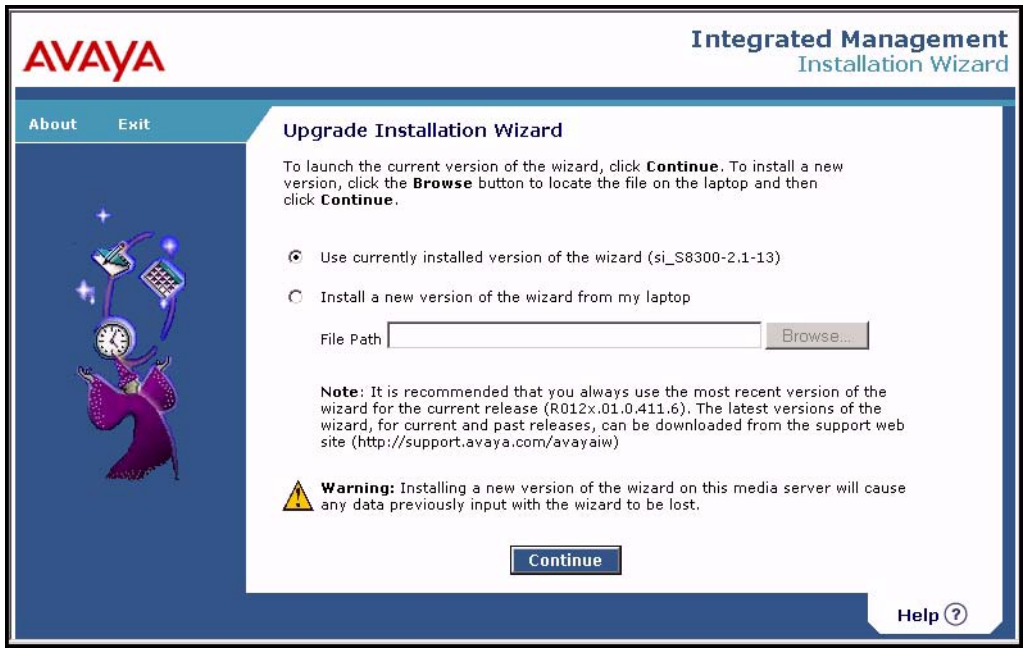
You should use the version of the Installation Wizard (IW) that corresponds to the release of Communication Manager you are upgrading ***from***. When you use the IW, you will be asked if you want to install the latest version of the IW from your laptop or from the Avaya Support website. Be sure not to install a version of the IW later than the version of Communications Manager from which you are upgrading. For example, if you are upgrading Communication Manager from release 2.2 to release 3.0, you cannot use the 3.0 version of the IW; you must use the 2.2 version.

Note:

Manual installation procedures can be found in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware

From the Maintenance Web Interface, launch the Avaya Installation Wizard. The **Upgrade Installation Wizard** screen displays. You can use the currently installed version of the IW, or you can choose to install a new version of the IW from your laptop.

Upgrade Installation Wizard screen

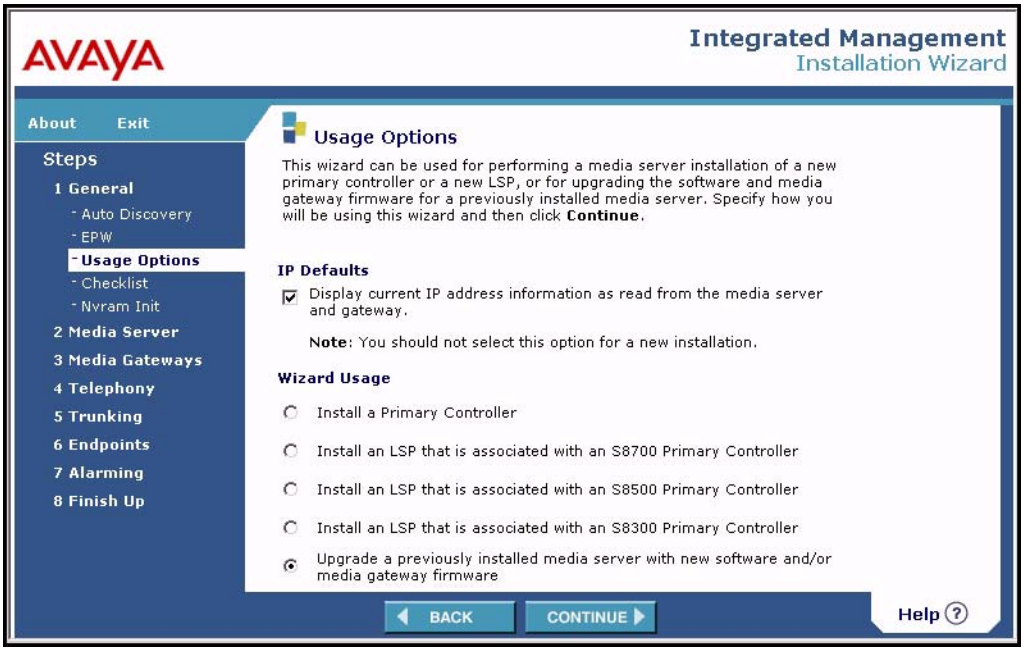


When you are finished with the Upgrade Installation Wizard screen, click **Continue**. Following brief **Overview** and **Auto Discovery** screens that display system data for the installation, such as:

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

the **Electronic Preinstallation Worksheet** screen displays. Because this is an upgrade of an existing media server and media gateway, click the **Continue** button. The **Usage Options** screen displays.

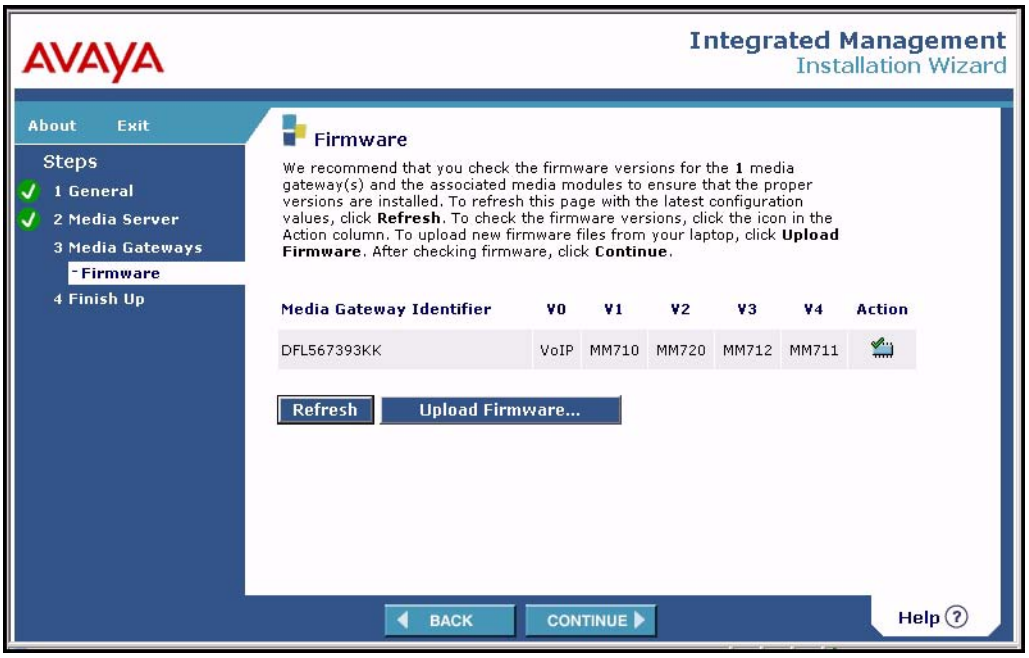
Usage Options screen



You can choose any of several **Wizard Usage** options. For an upgrade of an existing media server and media gateway, select the **Upgrade a previously installed media server with new software and/or media gateway firmware** radio button. Check the **IP Defaults** checkbox. When you are finished with this screen, click **Continue**.

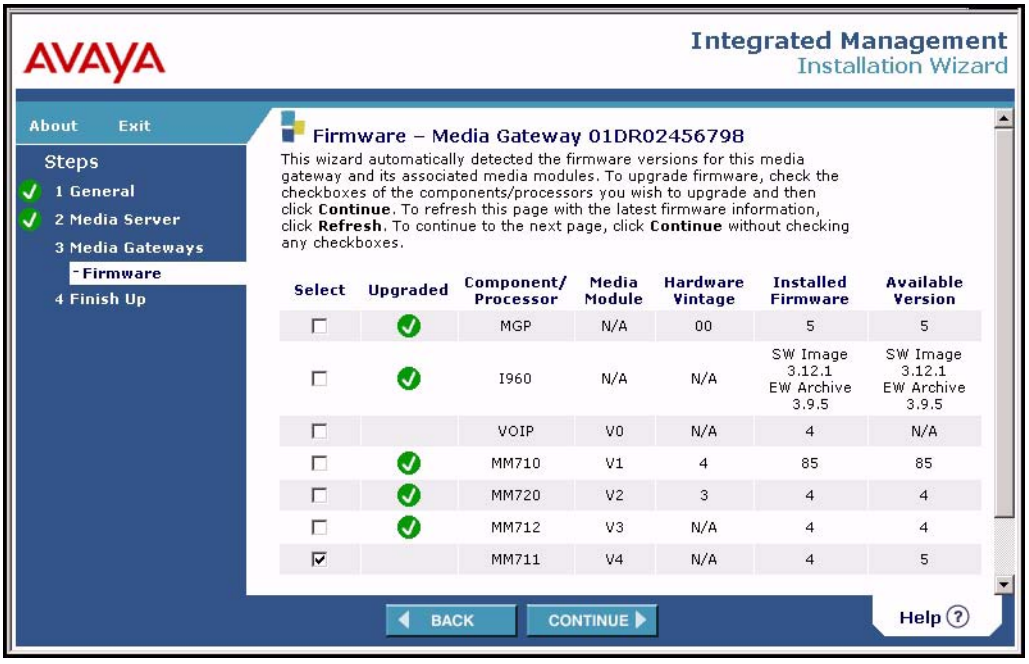
Click **Continue** to move through the **Media Server** tasks. The first **Media Gateway** screen to display is the **Firmware** screen.

Firmware screen



This screen displays the Media Gateway and its associated media modules. To check the installed compared to available versions of firmware, click on the icon in the **Action** column. The **Firmware - Media Gateway <identifier>** screen displays.

Firmware - Media Gateway <identifier> screen



In this example the screen shows the G700 Media Gateway Processor, the P330 Stack Processor, the VoIP processor, and installed media modules. The detected hardware vintages, and the installed and available firmware vintages are displayed. For those components that already have installed the latest available firmware vintages, a green check mark appears next to the component. If a more recent firmware vintage is available (in the S8300 Media Server *tftpboot* directory), you can select the checkbox at the left of the component. When you are finished, click **Continue**. The firmware on the checked component(s) is automatically upgraded. You are then returned to the **Firmware** screen.

Click **Continue**. Follow the instructions, as necessary, on the next few screens to **Finish Up** the upgrade of G700 firmware.

Upgrading G700 firmware using the upgrade tool from the primary controller

Note:

The Upgrade Tool must be run from the primary controller. The Upgrade Tool cannot be used on an S8300 configured as an LSP.

On the Integrated Management main menu, click **Launch Upgrade Tool**. Follow the instruction to upgrade the G700 and media module firmware. For more information on the Upgrade Tool, see *Job Aid: Upgrade Tool and Worksheets, 555-245-757*.

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 319

Completing the upgrade process (S8300 is the primary controller) on page 320

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.

To obtain the post-upgrade service pack file and documentation

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.

7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 software.

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 320
2. To enable scheduled maintenance on page 320
3. To busy out trunks on page 321
4. To check for translation corruption on page 321
5. To resolve alarms on page 321
6. To re-enable alarm origination on page 321
7. To back up the system on page 321
8. To restart LSPs (if any) on page 321

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 290).

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.

To restart LSPs (if any)

To restart Communication Manager on an LSP after the upgrade:

1. Open a Telnet session on the S8300 (LSP).
2. At the command line, type **start -ac** and press **Enter**.

This completes the upgrade process for a G700 with an S8300.

Chapter 7: Upgrading an existing G700 without an S8300

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 Manger. 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. Installing 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 47 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 325
- Getting the serial number of the G700, if necessary on page 325
- Setting up the TFTP server on your laptop or on a customer PC, if necessary on page 326
- Downloading G700 firmware files to your TFTP directory on page 326

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.

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, 1.3 to 2.1), you will need the serial number of the G700.

To get the G700 serial number

1. Ask the customer's administrator to log in to the S8300 Web page.
2. 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.

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 15:

   Note:

   The latest firmware versions may different from those listed in Table 15. 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.

Table 15: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_0_17.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.0.4.exe
G700 Media Gateway	mgp<version id>	mgp_21_16_0.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v43.fdl
8-port DCP Media Module	mm712<version id>	mm712v5.fdl
24-Port DCP Media Module	mm717<version id>	mm717v2.fdl
8-port/trunk Analog Media Module	mm711<version id>	mm711h20v60.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v60.fdl
T1/E1 Media Module	mm710<version id>	mm710v9.fdl
8-port BRI Media Module	mm720<version id>	mm720v4.fdl
2-port BRI Media Module	mm722<version id>	mm722v2.fdl

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.

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 328
- Verifying the contents of the tftpboot directory on page 329

as described in this section.

Accessing the P330 Stack Processor

See About connection and login methods on page 47 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   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 G700 Media Gateway

You can use the Upgrade Tool (running on the primary controller) to perform this task automatically. The Upgrade Tool can also be used to upgrade firmware on the G350.

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.

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 8: 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 334
- Complete the telephone installation process on page 360

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 362
- INTUITY AUDIX LX messaging system on page 364
- ASAI co-resident DEFINITY LAN gateway (DLG) on page 364
- Call center on page 366
- Avaya Integrated Management on page 369
- Uninterruptible power supply (UPS) on page 374
- Terminal server installation on page 376
- Call detail recording (CDR) on page 390
- Reliable Data Transport Tool (RDTT) package on page 394
- Printers on page 395
- DS1/T1 CPE loopback jack on page 396
- External modems on page 411
- Busy tone disconnect equipment for non-U.S. installations on page 413
- Music-on-hold on page 414
- Paging and announcement equipment on page 418
- Adjunct Information Sources on page 419

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 Manage*r, 03-300509. Refer to the *Installation for Adjuncts and Peripherals for Avaya Communication Manager,* 555-233-116*,* to install the necessary peripheral equipment

These references are on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

About connectable telephones and consoles

Table 16: 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 16: Connectable Telephone and Consoles

Telephone and Console Models	Type
46xx series:* 4601, 4602, 4606, 4610SW, 4612, 4620, 4620SW, 4624, 4690	Internet Protocol (IP)
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
62xx series: 6211, 6219	Analog

1 of 2

Table 16: Connectable Telephone and Consoles (continued)

Telephone and Console Models	Type
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

*. For information on administering 46xx series IP Telephones, see *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507.

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 17 shows a pinout chart for two-wire stations.

Table 17: 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 18: 2500-Type Analog Telephone Wiring

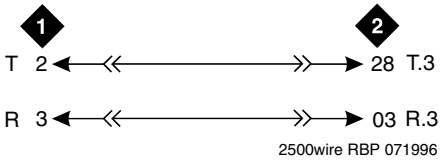


Figure notes:

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 77) 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.

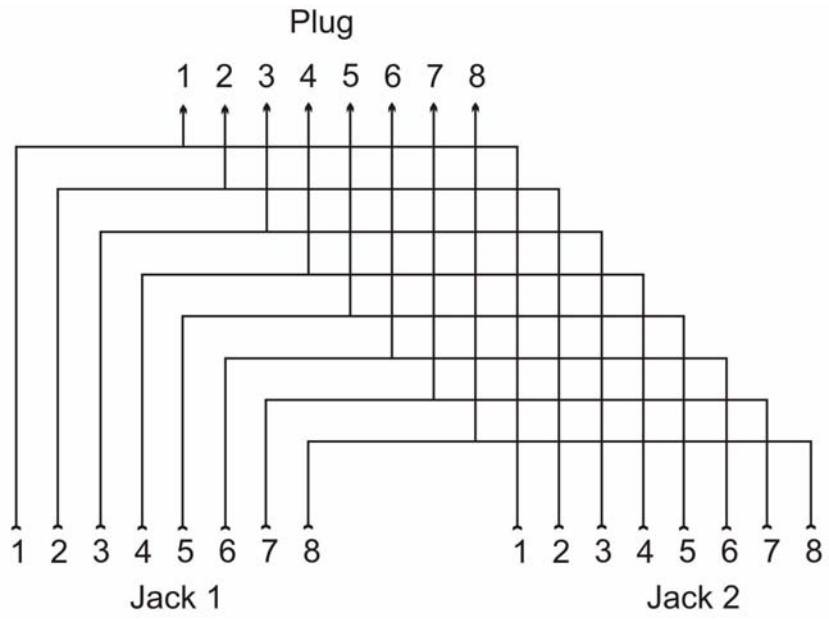
To connect one ISDN BRI station to one ISDN port:

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 19 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 19: 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 20: 808A Emergency Transfer Panel on page 339.

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 20: 808A Emergency Transfer Panel

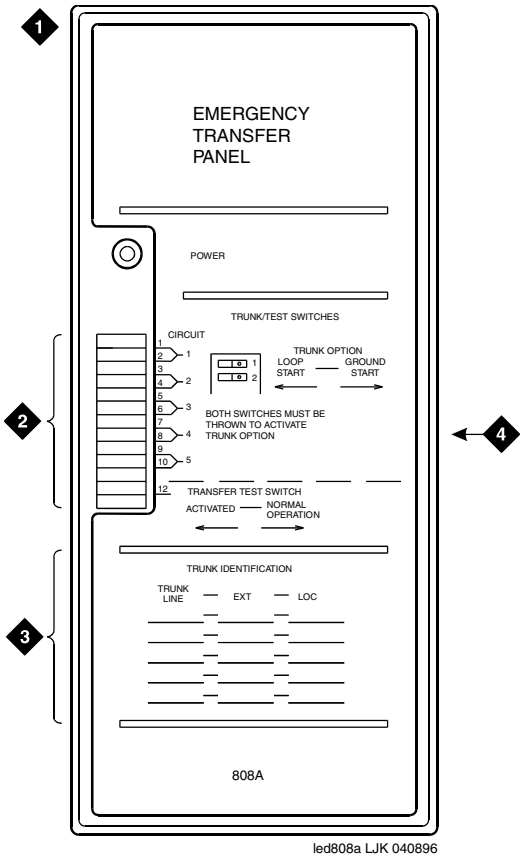


Figure notes:

1. **808A emergency transfer panel**
2. **Circuit start selection switches**
3. **Trunk identification label**
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.

Note:

Refer to the *Installation for Adjuncts and Peripherals for Avaya Communication Manager,* 555-233-116*,* to install the necessary peripheral equipment.

The power is provided to telephones or consoles either centrally or locally.

Centrally located power supplies include:

- 1152A1 mid-span power distribution unit on page 343
- P333T-PWR power over ethernet stackable switch on page 356

Local power supplies include:

- 1151B1 and 1151B2 power supplies on page 347

Typical adjunct power connections

The 400B2 adapter is convenient for connecting local -48 VDC power to a modular plug. See Figure 21: 400B2 Adapter Connecting to a Modular Plug on page 341.

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 1151A1 or 1151A2 power supply. The 1151A1 is a standard (no battery backup) power supply unit. The 1151A2 is a battery backup version of the 1151A1. 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 21: 400B2 Adapter Connecting to a Modular Plug

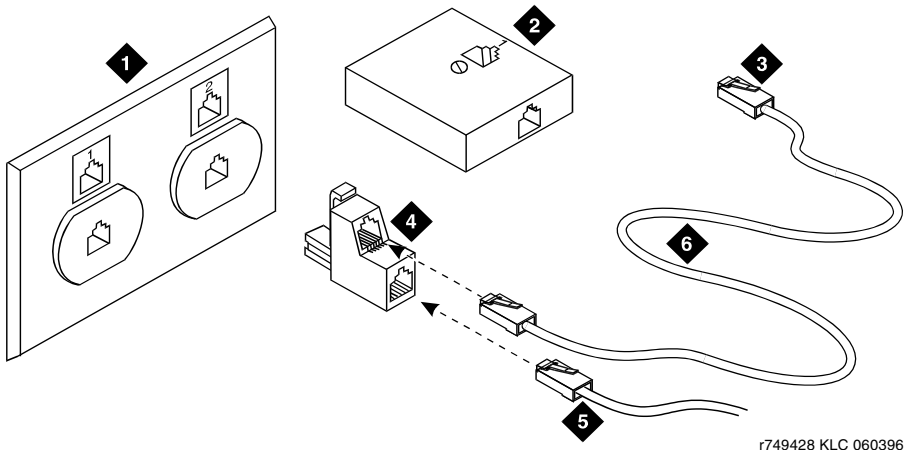


Figure notes:

1. **Flush-Mounted Information Outlet**
2. **Surface-Mounted Information Outlet**
3. **To Individual Power Unit**
4. **400B2 Adapter**
5. **To Telephone**
6. **Destination Service Access Point (DSAP) Power Cord**

Typical adjunct power connections end-to-end

Figure 22: Example Adjunct Power Connections on page 342 shows typical connection locations for adjunct power.

Figure 22: Example Adjunct Power Connections

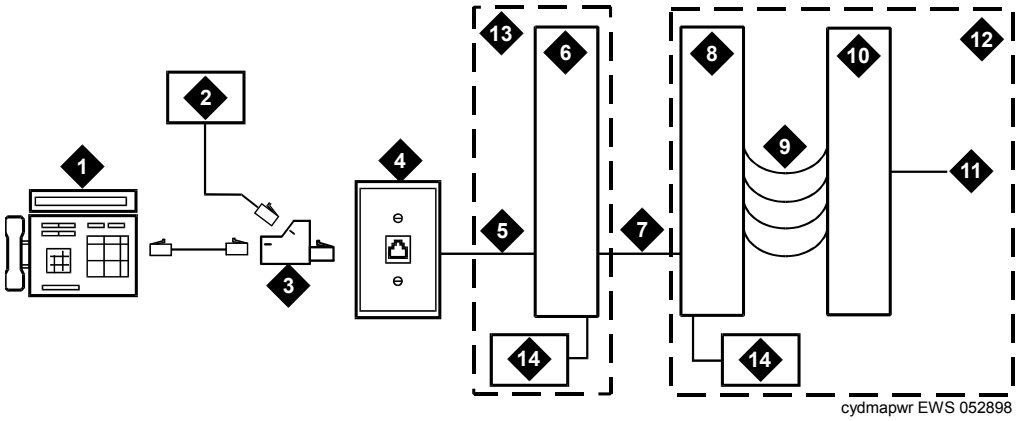


Figure notes:

1. **Typical display telephone**
2. **Individual power supply (Such as 1151B) (Not used if item 14 is used)**
3. **400B2 adapter**
4. **Information outlet (modular jack)**
5. **4-pair D-Inside Wire (DIW) cable**
6. **Satellite site or adapter location**
7. **25-pair D-Inside Wire (DIW) cable**
8. **Station side of MDF**
9. **100P6A patch cord or jumpers**
10. **System side of MDF**
11. **25-pair cable to digital line modular jack**
12. **Equipment room**
13. **Satellite location**
14. **Bulk power supply. Install at satellite location or equipment room (not both).**

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 or 1151B2 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 18: Attendant Console Cabling Distances on page 343.

Table 18: 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 unit

The 1152A1 Mid-Span Power Distribution Unit (PDU) is an Ethernet power supply that provides power to up to 24 46xx-series IP telephones or wireless LAN (WLAN) access points. This unit is used with a 10/100BaseTx standard Ethernet network over a standard TIA/EIA-568 Category 5, 6 or 6e cabling plant. The 1152A1 meets 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 19: 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 344. For installation instructions, see Connecting the 1152A1 PDU cables on page 345.

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 24, 10/100 Base-T ports, 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.

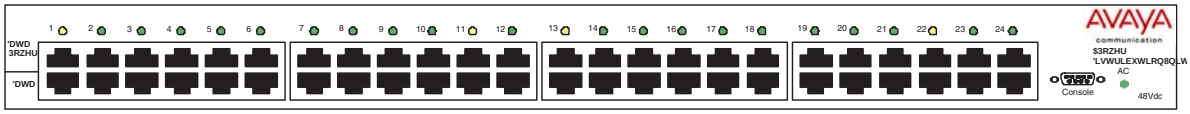
1. Plug a power cord into the power socket on the rear of the 1152A1 Power Distribution Unit.
2. Plug the other end of the power cord into the power receptacle.

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.

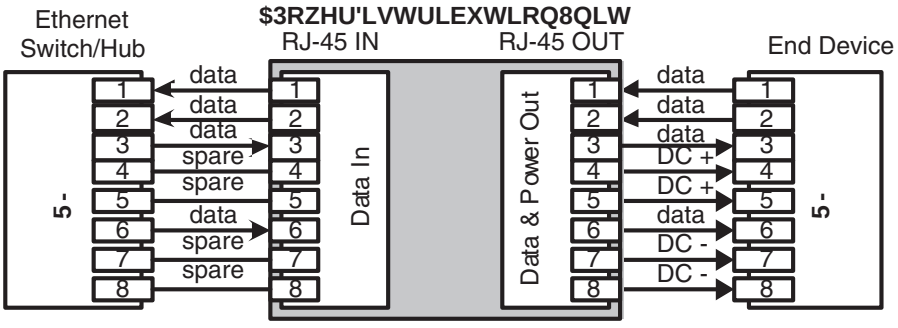
Connecting the 1152A1 PDU cables

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 346.

Figure 23: 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.

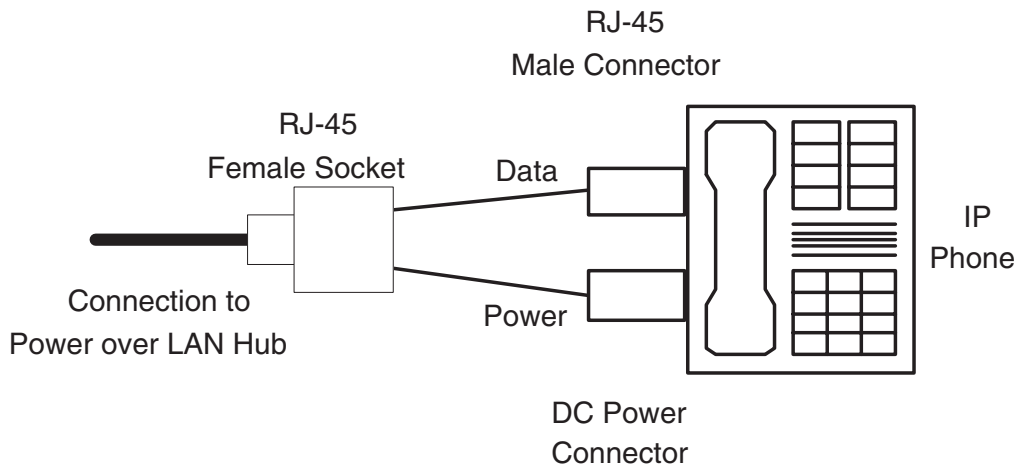
Connecting cables to telephones and other end devices

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 24: Connecting an IP telephone with an external splitter on page 346).

Figure 24: 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.

1151B1 and 1151B2 power supplies

The 1151B1 and 1151B2 power supplies are local power supplies. The telephones or consoles connect directly to them through an RJ45 connector. The 1151B2 has a battery backup.

These power supplies comply with the Underwriters Laboratories Inc. (UL) Standard UL 60950 third edition.

Table 20: 1151B1 and 1151B2 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 and 1151B2 power supplies on page 347. For installation instructions, see Connecting the 1151B1 or 1151B2 power supplies on page 349.

Important safety instructions for 1151B1 and 1151B2 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 and 1151B2 power supplies

The 1151B1 and 1151B2 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:

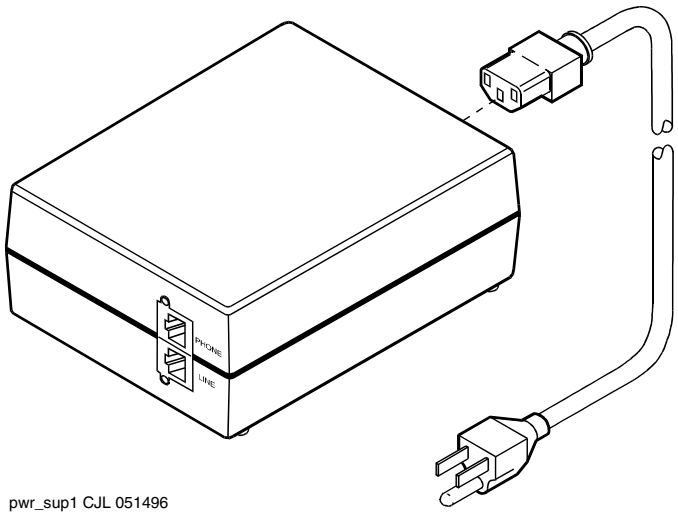
Do not locate the unit within 6 inches (15 centimeters) of the floor.

Connecting the 1151B1 or 1151B2 power supplies

The 1151B1 is a standard (no battery backup) power supply unit. The 1151B2 is a battery backup version of the 1151B1. 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 25: 1151B2 Power Supply — Front on page 349.

Figure 25: 1151B2 Power Supply — Front



Avaya Power over Ethernet (PoE) switches

Available PoE Switch Options

Data and power are combined in a (PoE) switch and sent over a single cable, thus simplifying power management and cabling infrastructure and saving rack space.

Avaya offers the following PoE switches:

- C360 Converged Stackable Switches (C363T-PWR and C364T-PWR)
- C460 Converged Multilayer Switch
- P333T-PWR PoE Switch

All PoE Switches comply with the IEEE 802.3af standard.

Switch	Maximum PoE Power (W)	Number of Powered Ports in Switch
C363T-PWR	305	24
C364T-PWR	520	48
C460	2,400 (with three PSUs)	192
P333T-PWR	200	24

PoE is carried over the signal leads, providing remote -48V power feeds on all 10/100 ports in the switch/module (except on an expansion module in P333T-PWR). This allows the PD (Powered Device) to be up to 100m away from the switch. Each port performs a standard compatibility detection process before power is supplied to the Ethernet lines. If the PD is removed or the link is interrupted, the port polling mechanism detects this, and power is cut off to the port while the detection process is applied again.

The PoE switch applies power to the port only after it detects that a PD is actually connected to the port. Each PD has a resistance range known as a "signature." The switch knows what power has to be supplied to the device according to the signature.

Load detection is performed every 240 ms. All ports are checked for the resistance signature on a port-by-port basis. Only non-powered ports participate in the periodic load detection. Once power is provided to a port, it is checked periodically to see if a PD is still connected. If a PD is disconnected from a powered port, then power is denied to the port. Disconnected ports then automatically join the periodic load detection cycle. Each port of the switch is protected against channel overload, short circuit, and reversed polarity that might be caused by faulty connection between two feeding channels or by a crossed cable connection.

Power priority mechanism

The priority mechanism is implemented in order to handle cases where the power requested by the PDs exceeds the switch PoE capacity. This priority mechanism determines the order in which ports will be powered on after boot, and powered off if the power resources of the module are exhausted. Three user-configurable port power priority levels are available: low, high & critical. Within each priority level the lower the port number, the higher the priority (by default all the ports have low priority).

Disconnected power will be automatically reconnected to the PDs based on their priority, whenever there is an available power budget. Immediately after the PoE has booted up, it starts to supply power to the ports where a load is detected. Ports are powered up one after another, based on the port priority, until the limit is reached. Power calculation is based on the actual power consumption of the PD. After this, no more ports are powered up until the total power consumption drops lower than the limit. The limit is 18 Watts below the maximum PoE capacity. The remaining 18W are reserve power for a change in the power draw of PDs.

C360 converged stackable switches

The Avaya C360 converged stackable switch series is a line of stackable, multilayer switches that provide high availability, quality of service (QoS), and Power over Ethernet (PoE) to enhance converged network infrastructure operations. With a range of PoE and non-PoE configurations, the C360 series is a powerful, yet cost-effective option for enterprise applications. The C360 series offers a migration path for the P330 series, and can be stacked with P330 switches and G700 Media Gateways.

The Avaya C360 series of converged stackable switches includes:

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

The available C360 switch models are as follows:

- C363T converged stackable switch

  This switch has 24 10/100 Mbps ports and two GBIC SFP ports.

Figure 26: C363T Converged Stackable switch

- C363T-PWR converged stackable switch

  This switch has 24 10/100 Mbps ports with Power over Ethernet (PoE) and two GBIC SFP ports.

Figure 27: C363T-PWR Converged Stackable switch

- C364T converged stackable switch

  This switch has 48 10/100 Mbps ports and two GBIC SFP ports.

Figure 28: C364T Converged Stackable switch

- C364T-PWR converged stackable switch

  This switch has 48 10/100 Mbps ports with Power over Ethernet (PoE) and two GBIC SFP ports.

Figure 29: C364T-PWR Converged Stackable switch

A C360 switch can co-reside in a stack with G700 media gateways and with selected P330 switches. A C360 stack can contain up to 10 switches and up to three backup power supply units. The stacked switches connect using the stacking sub-modules that plug into a slot in the back of the C360. The 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.

Avaya C360 switches are multilayer switches and can be upgraded with a license to provide routing (Layer3) functionality.

Features of the C360 converged stackable switches

The C360 Converged Stackable switches offer features in the following categories:

- Stacking
- Layer 2 features
- Layer 3 features
- Management
- Power over Ethernet (PoE)

Stacking

- Up to 10 switches can be stacked together.
- Features such as Spanning Tree, redundancy, VLANs, and SMON are common to the stack.

- The Octaplane stacking system provides 8 Gbps stacking bandwidth to all switches in the stack.
- C360 stacks continue to function even if one switch or link fails.
- Switches in the stack can be added, removed, and replaced without disrupting operation.
- An advanced election algorithm ensures optimal stack master selection.

Layer 2 features

- Auto-sensing simplifies configuration of LAN connections by automatically selecting the port speed for devices — either 10Mb or 100Mb.
- Auto-negotiation simplifies configuration of LAN connections by automatically selecting the port transmission mode for devices — either half- or full-duplex.
- Auto-MDIX automatically adjusts for straight-through or crossover cables on all 10/100-TX ports.
- Traffic prioritization (802.1p) allows real-time traffic classification into 8 priority levels mapped to 4 queues.
- There are four egress queues on all switch ports. The queues can be configured with the WRR (Weighted Round Robin) or strict priority scheduling algorithm.
- The use of the IEEE 802.1Q tagging for VLANs and per-port VLAN is supported.
- Multiple VLANs per port allow access to shared resources by stations that belong to different VLANs.
- The use of the IEEE 802.1w standard for Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree in case of link failure.
- The use of the IEEE 802.1x standard for port-based network security ensures that only authorized clients get network access.
- Up to 20 redundant-port pairs are supported to increase link resiliency.
- Inter-module redundancy is supported with one pair in a stack. The switching time is approximately 1 second.
- Link Aggregation Group (LAG) support of up to 7 trunks, with each trunk having up to 8 10/100 links or 2 GB links, provides resiliency, load balancing, and bandwidth expansion.
- LAG redundancy is supported through resiliency between two LAG groups.
- Port mirroring of any switch port is supported.
- RMON/SMON port statistics provide real-time top-down analysis of network traffic.
- IP multicast filtering (snooping) filters multicast traffic to optimize network bandwidth.
- Classification of ports as regular or valuable is supported so that if a link fails, notification is generated for valuable ports only.
- The L2 CAM table contains 16K MAC addresses.

Layer 3 features

Note:

An additional license is required for Layer 3 features.

- Static, RIPv1, RIPv2, OSPF IP routing protocols are supported.
- Equal cost routing is used for load balancing and redundancy.
- Router redundancy (VRRP) is supported.
- NetBIOS rebroadcasting is available for applications such as WINS that use broadcasting but may need to also communicate with stations on other subnets or VLANs.
- ICMP and ARP protocols are supported.
- DHCP/BootP relay allows broadcast requests to be forwarded to servers.
- Policy-based routing of packets provides enforcement of QoS and ACL rules.
- The L3 CAM table contains 4K IP addresses.

Management

- Access to the management interfaces are password-protected at three levels (read-only, read-write access and supervisor) to prevent unauthorized configuration changes.
- You can access to the Command Line Interface (CLI) in the following ways:
  - Direct console or modem connection
  - Telnet (up to five simultaneous connections) or SSHv2 (up to two simultaneous connections) over the IP network
- You can use TFTP for the download/upload of configuration files or the download of firmware files
- You can use SCP (Secure Copy Protocol) for secure download/upload of configuration files
- You can use SSH encrypted login sessions as a secure way to manage the switches remotely.
- A Java-based Device Manager provides an intuitive Web-based interface for access
- SNMPv1 is supported.
- Simple network time protocol (SNTP) or TIME protocols are available to provide a consistent timestamp to all switches from an external source.
- Radius authentication enables centralized user management.
- You can use all appropriate tools of the Avaya Integrated Management suite for administration.
- System logging can occur by terminal, internal file, or Syslog server.
- Switch access can be restricted to specified protocols or services.

- You an restrict access to management interfaces by IP address.
- You can invoke a telnet client from the CLI.

Power over Ethernet (PoE)

- PoE is supported on the C363T-PWR and C364T-PWR switches.
- PoE is fully compliant with the 802.3af-2003 standard.
- PoE provides up to 15.4W per port (on10/100 ports) over Ethernet cables to power IP phones, wireless access points, and other end-points using 802.3af-2003 standards.
- PoE automatically detects device connections and removal.
- PoE automatic load detection does the following:
  - Tests whether the device connected to the port requires remote powering.
  - Controls the power injection to the wires.
- Power is distributed between the 24/48 PoE ports according to priorities that you configure. Power priority can be configured on each port. Distribution is calculated from actual power consumption.

C460 converged multi-layer switch

For enterprises looking to deploy Avaya Communication Manager Communications Applications, the Avaya C460 converged multi-layer switch is a highly resilient network platform designed to provide high-availability support for mixed data and IP Telephony deployments.

The Avaya C460 features a compact modular six-slot chassis with the following main characteristics:

- Four I/O slots and two Supervisor slots
- Fully redundant architecture (including switching fabric, supervisor modules and PSUs)
- Power over Ethernet (PoE) support with the FE ports
- High density - up to 192 FE PoE ports and 48 GE ports
- Fabric switching throughput of 64Gbps at Layer 2 and 48Mpps routing at Layer 3
- Policy and QoS mechanisms
- Full router functionality
- Wire-speed Layer 3 forwarding on all ports
- Optimal use of physical chassis size (10U)
- 300W or 1000W (for PoE support) power supplies

The C460 full redundancy (supervisor and fabric, power supply, link and port interfaces, router processor, and fans), high port density and powerful Layer 2 and Layer 3 wire-speed switching engine make it suitable for robust network infrastructure. The C460 offers advanced management and monitoring capabilities using complete GUI tools, including the SMON and Any-layer SMON applications in the Avaya Information Management software.

The C460's available I/O modules include:

- 48 10/100 PoE port Inline Power module
- 48 10/100 PoE port Inline Power + 2 GBIC (SFP) Gigabit Ethernet port module
- 12 GBIC (SFP) ports Gigabit Ethernet module
- 48 10/100 port Ethernet module
- 48 10/100 port Ethernet + 2 GBIC (SFP) Gigabit Ethernet port module

The C460 extends Avaya Convergence solutions to the network edge by providing advanced network capabilities, including Quality of Service (QoS), high performance, advanced power management, security and manageability. Designing a converged network infrastructure using this highly-resilient, modular, high-performance solution ensures a lifespan of the network, which reduces the cost of ownership and improves return on investment.

With its flexible configuration options and high-capacity performance, the C460 can also be deployed as a distribution layer switch or as the network backbone for small to medium enterprises looking for a reliable modular solution.

For enterprises deploying Avaya Communications Manager for mission-critical call center and large-scale campus environments, the C460 offers an ideal IP Telephony platform that combines fault tolerance, network responsiveness for business continuity, and integrated management and monitoring for converged networks.

P333T-PWR power over ethernet stackable switch

The P333T-PWR power supply complies with the Underwriters Laboratories Inc. (UL) standard UL 1950, second edition.

Table 21: P333T-PWR UL 1950 Compliance

Complies	UL 1950
Approved	C22.2 No.950 Std.
Approved	CE

For safety instructions, see Important 1152A1 PDU Safety Instructions on page 344. For installation instructions, see Connecting the P333T-PWR switch on page 358.

Important P333T-PWR switch 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 Avaya P333T-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 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 P333T-PWR switch

The P333T-PWR Power over Ethernet Stackable Switch can be used to power 46xx series IP telephones in addition to providing a 10/100 megabits per second Ethernet connection. The switch can form part of a stack with the G700 Media Gateway or members of the P330 stackable switching system.

CAUTION:

The Avaya P333T-PWR switch does not contain any user-serviceable components inside. Do not open the case.

CAUTION:

The P333T-PWR switch can be used only indoors and in a controlled environment.

The P333T-PWR switch has 24, 10/100 Base-T ports, each of which can supply up to 16.5 watts using the internal power supply and operates on a 100–240 volts AC, 5.3 amperes, 50/60 hertz power source with the option of using the 44~57 volts DC, 15 amperes to boost the inline power.

The P333T-PWR switch can be placed in a wiring closet or on a flat, stable surface like a desk. Screws are provided for mounting in a standard 19-inch rack.

Connecting the P333T-PWR switch

To power up—AC input

1. Insert the power cord into the power connector (BUPS or AC Power Supply) on the rear of the unit. See Figure 30: Connectors on the P333T-PWR switch on page 358.

Figure 30: Connectors on the P333T-PWR switch

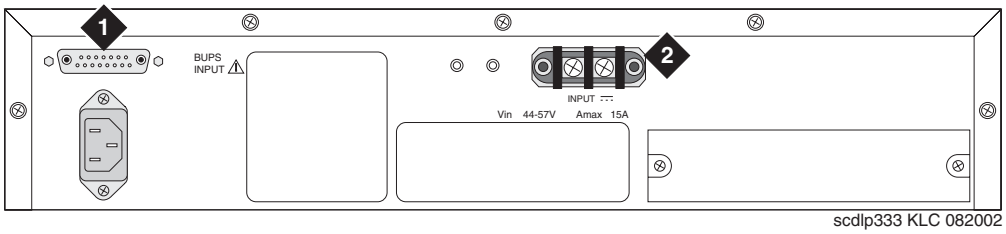


Figure notes:

1. **BUPS connector**
2. **AC connector**

2. Insert the other end of the power cord into a non-switched electrical 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.

To power up—DC input (optional)

The P333T-PWR switch can operate on the AC input only. However, you may wish to use the optional DC input for the following:

- To backup the power over Ethernet ports
- To provide more than 200 watts for the power over Ethernet ports

Note:

Please refer to the P333T-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 P333T-PWR switch.

   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 P333T-PWR switch to a switch or hub.

3. Check that the appropriate link (LNK) LEDs light up.

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 360
- Installing over-voltage and sneak-current circuit protection on page 361

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 mm^2) 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 22: Ethernet Interfaces summarizes Ethernet interfaces used by several current switching platforms:

Table 22: 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 23: Comparison between the G700 Announcement software and the VAL circuit pack on page 367 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 23: 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 23: 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 MultiService Network Manager
- 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 MultiService Network Manager

Avaya MultiService Network Manager 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 MultiService Network Manager 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 MultiService Network Manager, 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 MultiService Network Manager 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 MultiService Network Manager.

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 Vac[3], 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 Guide 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 31: 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 31: Switch-to-adjunct LAN connectivity through a terminal server

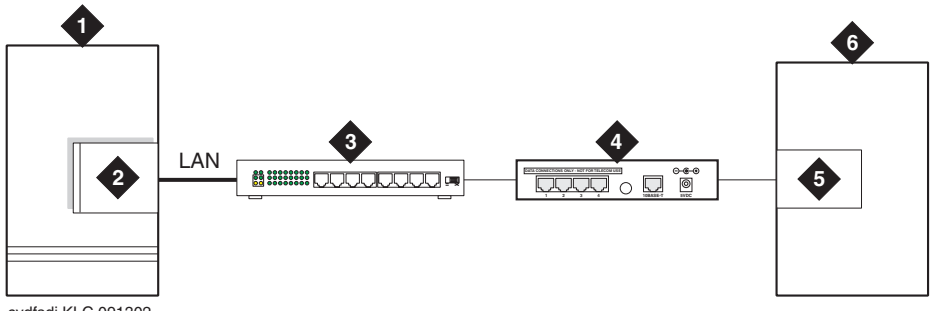


Figure notes:

1. **switch**
2. **IP connection on an S8300/G700 or G350 configuration**
3. **10/100Base-T Hub (optional)**
4. **terminal server**
5. **serial port**
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 24: Required equipment.

Table 24: 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 24: 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

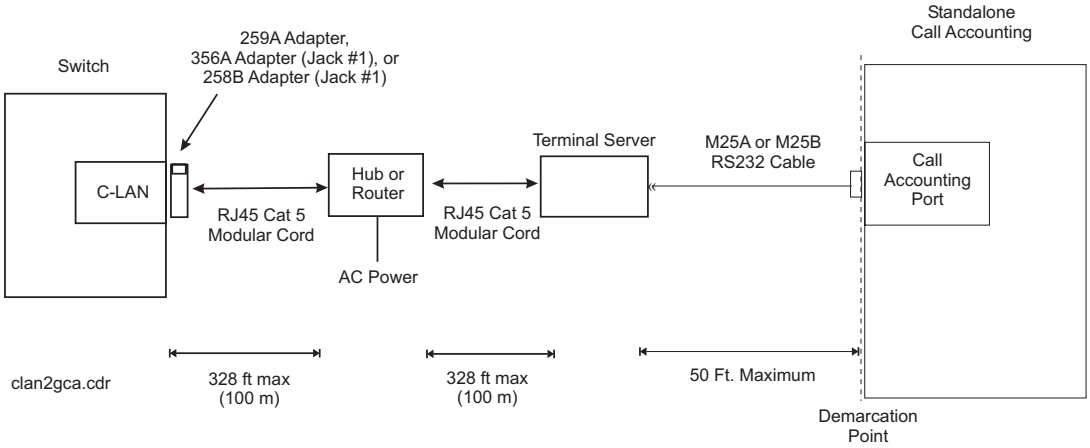
The distance limit from the switch to the LAN hub is 328 feet (100 meters). The distance limit from the LAN hub to the terminal server is 328 feet (100 meters). If installed, the limit from the terminal server to the adjunct is 50 feet (15 meters).

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 32 shows the connection between the terminal server port and a call accounting system.

Figure 32: 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 378
- Administering the IOLAN+ on page 379
- 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 33.

Figure 33: Connecting an adjunct to the IOLAN+

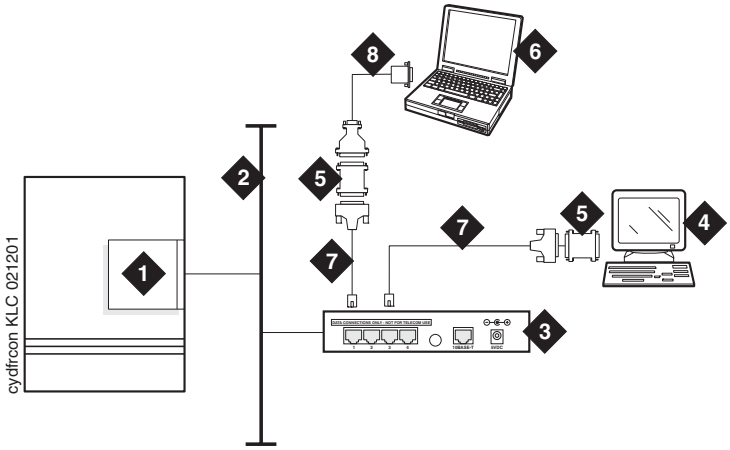


Figure notes:

1. **IP connection on an S8300/G700 or G350**
2. **Local area network (LAN)**
3. **IOLAN+ 104 terminal server**
4. **Adjunct (system management terminal or a system printer, for example)**
5. **Null modem**
6. **PC or laptop (for initial administration)**
7. **DB25-to-RJ45 cable**
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 ** === Commands ===
                            2            *** FREE ** | Telnet     ^T|
                            3            *** FREE ** | Rlogin    ^R|
                            4            *** FREE ** | 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.

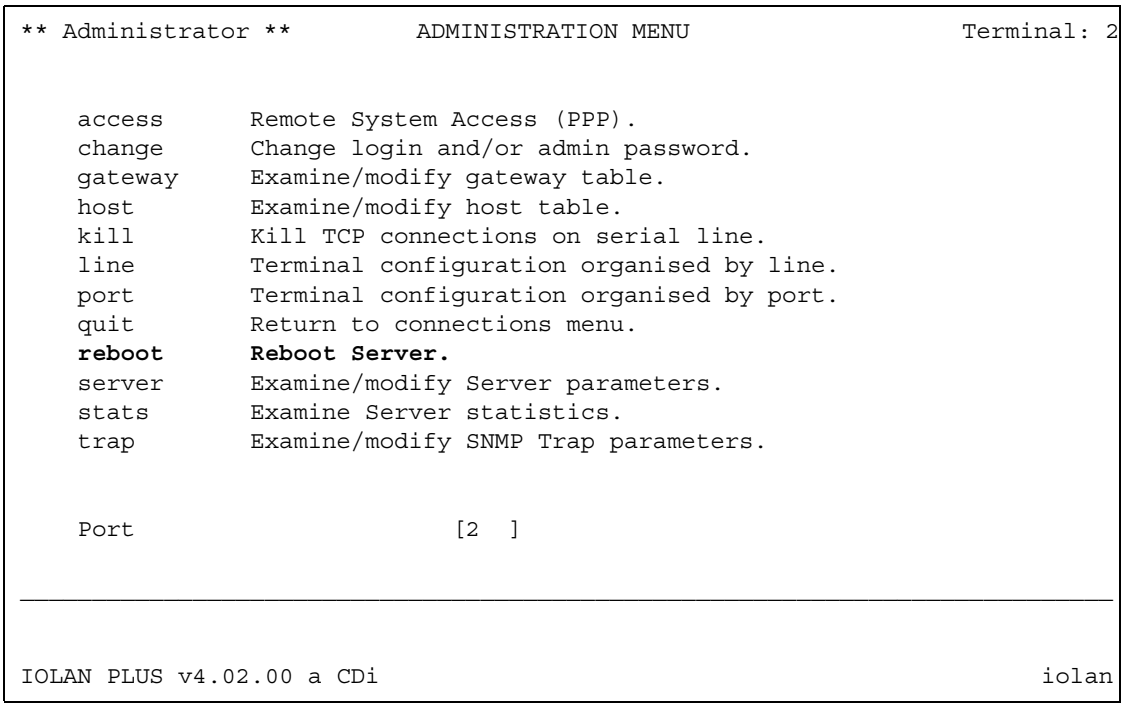
   - **Name:**
   - **IP address:** (for IOLAN+)
   - **Subnet mask:**

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**.



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 33: Connecting an adjunct to the IOLAN+ on page 379).

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**

- **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 383 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 on page 426 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 388), 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 391.

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  Attendant Call Recording? 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
      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*, 03-300191.

```
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 376 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 396

Administering a loopback jack on page 398

Testing a loopback jack with a smart jack on page 398

Testing a loopback jack without a smart jack on page 407

Configurations using fiber multiplexers on page 410

Installing a loopback jack

You can use one of two installation options:

- Installing a loopback jack with a smart jack on page 396
- Installing a loopback jack without a smart jack on page 397

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 34.
- If there is an extended demarcation point and the smart jack is not accessible, install the loopback jack as shown in Figure 35.
- If there is an extended demarcation point, but the smart jack is accessible, install the loopback jack as shown in Figure 36.

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 34 through Figure 36.
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 37 and Figure 38.

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 37 through Figure 38.
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 34 through Figure 36).

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 25: DS1 Troubleshooting to troubleshoot.

Table 25: DS1 Troubleshooting

Condition	Solution
The value of the **Test: cpe-loopback-jack** field is `Pattern 3-in-24`	The loopback jack test is active.
The value of the **Synchronized** field is `N`	Retry the test 5 times.
The value of the **Synchronized** field remains `N` 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 *non-zero*	Repeat Step 1 several times.
The value of the **Synchronized** field is `Y`	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 25: 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 26: DS1 Bit-error count troubleshooting on page 401 to troubleshoot.

Table 26: 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 cpe-loopback-jack-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 27: Evaluation of DS1 loopback test results on page 402 to evaluate the test results and to determine the solution.

Table 27: 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 **`reset board`** ***`XXXVS`***.
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 34 through Figure 36).
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 400.

   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 34: Network interface at smart jack for an MM710 multi-media module

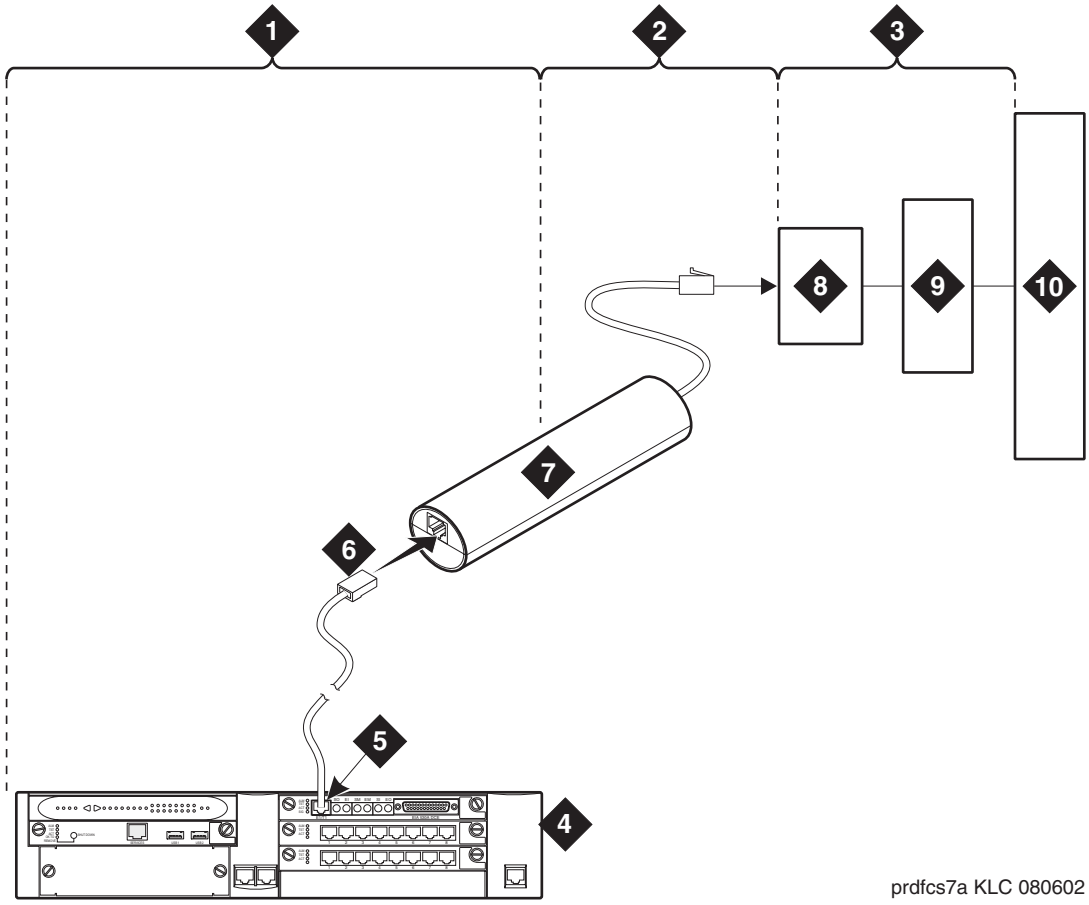


Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **Span section 3**
4. **G700 or G350 Media Gateway**
5. **E1/T1 port on an MM710 multi-media module**
6. **RJ-48 to network interface (up to 1000 ft. [305 m])**
7. **Loopback jack**
8. **Network interface smart jack**
9. **Interface termination or fiber multiplexer (MUX)**
10. **Central office**

Figure 35: Network interface at extended demarcation point (smart jack inaccessible) for an MM710 multi-media module

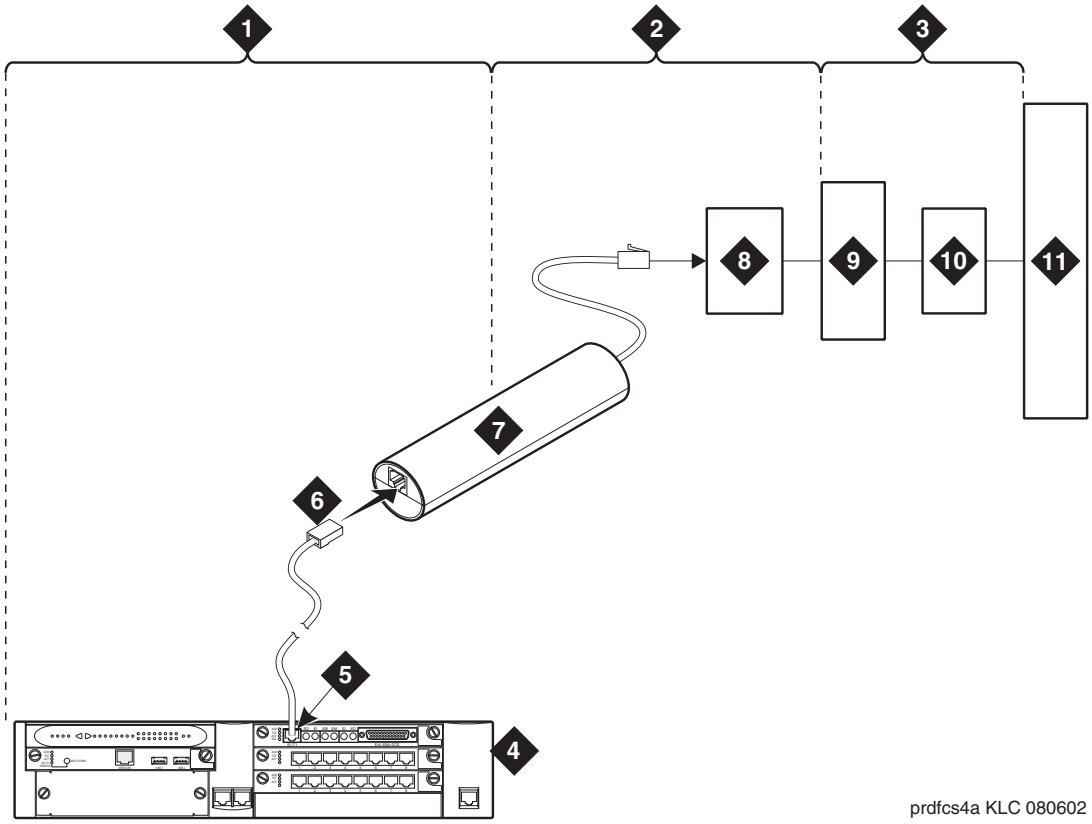


Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **Span section 3**
4. **G700 or G350 Media Gateway**
5. **E1/T1 port on an MM710 multi-media module**
6. **RJ-48 to network interface (up to 1000 ft. [305 m])**
7. **Loopback jack**
8. **Dumb block (extended demarcation)**
9. **Network interface smart jack**
10. **Interface termination or fiber multiplexer (MUX)**
11. **Central office**

Figure 36: Network interface at extended demarcation point (smart jack accessible) for an MM710 multi-media module

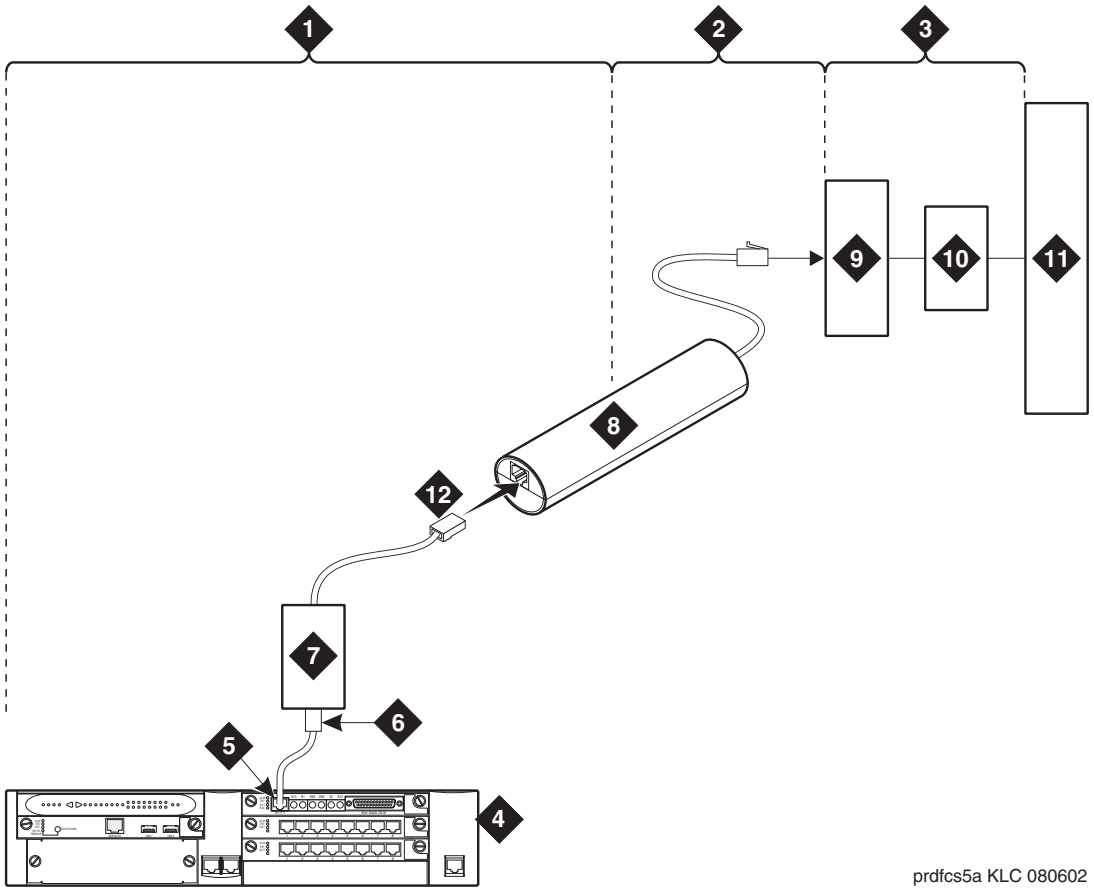


Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **Span section 3**
4. **G700 or G350 Media Gateway**
5. **E1/T1 port on an MM710 multi-media module**
6. **RJ-48 to network interface (up to 1000 ft. [305 m])**
7. **Dumb block (extended demarcation)**
8. **Loopback jack**
9. **Network interface smart jack**
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 37 and Figure 38.

Figure 37: Network interface at "dumb" block for an MM710 multi-media module

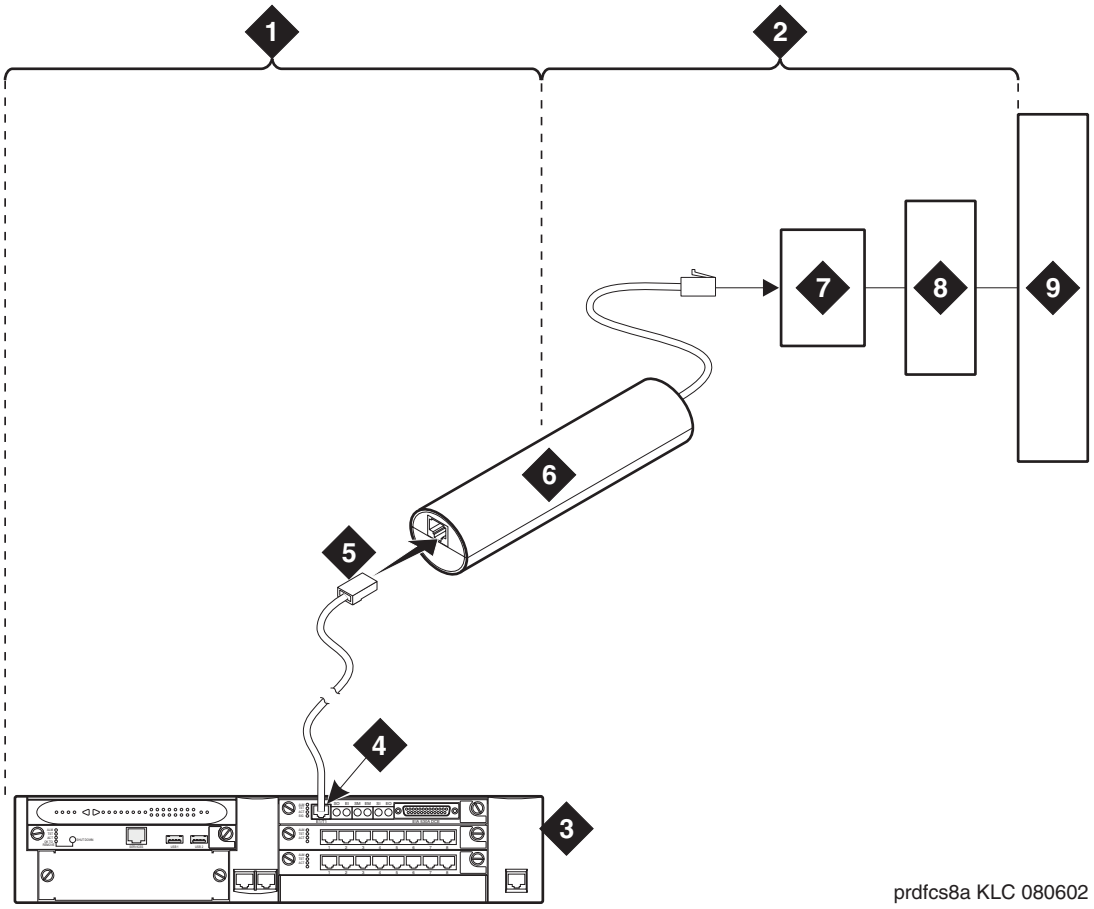


Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **G700 or G350 Media Gateway**
4. **E1/T1 port on an MM710 multi-media module**
5. **RJ-48 to network interface (up to 1000 ft. [305 m])**
6. **Loopback jack**
7. **Dumb block (demarcation point)**
8. **Interface termination or fiber multiplexer (MUX)**
9. **Central office**

Figure 38: Network interface at "dumb" block with repeater line to fiber MUX for an MM710 multi-media module

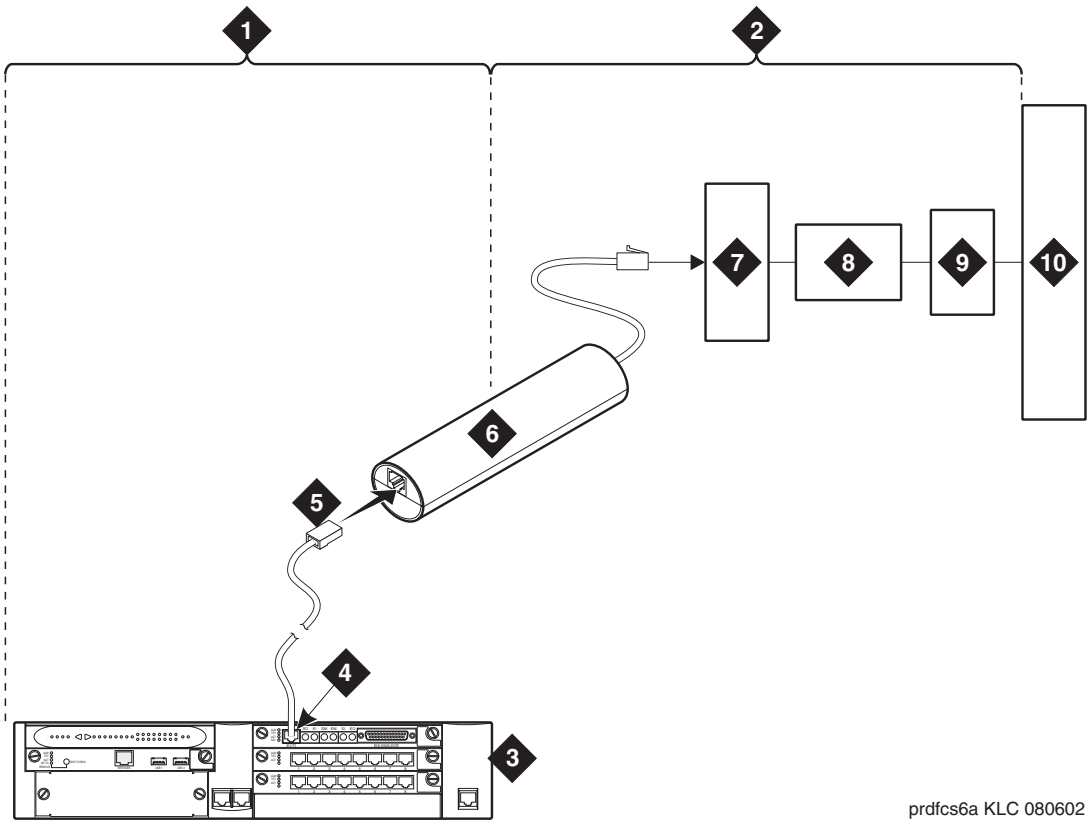


Figure notes:

1. **Span section 1**
2. **Span section 2**
3. **G700 or G350 Media Gateway**
4. **E1/T1 port on an MM710 multi-media module**
5. **RJ-48 to network interface (up to 1000 ft. [305 m])**
6. **Loopback jack**
7. **Dumb block (demarcation point)**
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 403.
2. Test the loopback jack-to-*dumb* block and *dumb* block-to-CO wiring (section 2 in Figure 37 and Figure 38).

   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 398. 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 34 through Figure 37. 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 411
- Multi-Tech MT5634ZBA-USB-V92 on page 411
- Multi-Tech MT5634ZBA-V92-GLOBAL on page 412
- Administering Multi-Tech modems on page 412

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 *Installation of the Avaya G350 Media Gateway Controlled by an Avaya S8300, S8500, or S8700 Media Server,* 555-245-104.

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 39 shows typical connections.

Figure 39: Typical cabling for busy tone disconnect

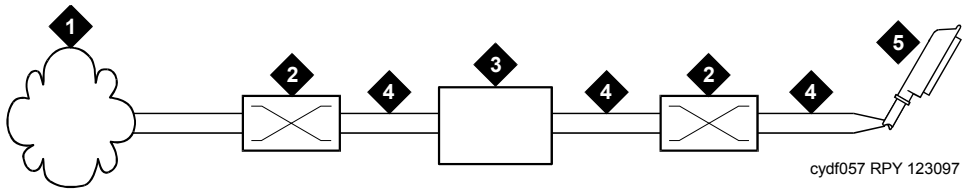


Figure notes:

1. **Public switched telephone network**
2. **Main distribution frame**
3. **Busy tone disconnect device**
4. **Tip and ring wires**
5. **To loop-start, central-office, trunk 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 414
- Installing a registered music source on a G700 or G350 Media Gateway on page 417

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 40 and Figure 41 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 40: Unregistered music-on-hold equipment connecting to KS-23395-L3 for a G700 Media Gateway

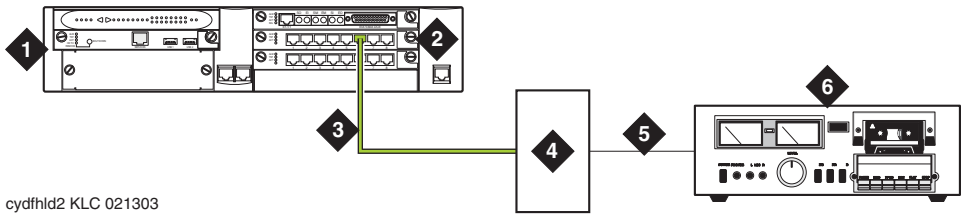


Figure notes:

1. **G700 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **KS-23395-L3 coupler**
5. **RCA cord**
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 41: Unregistered music-on-hold equipment connecting to KS-23395-L4 for a G700 Media Gateway

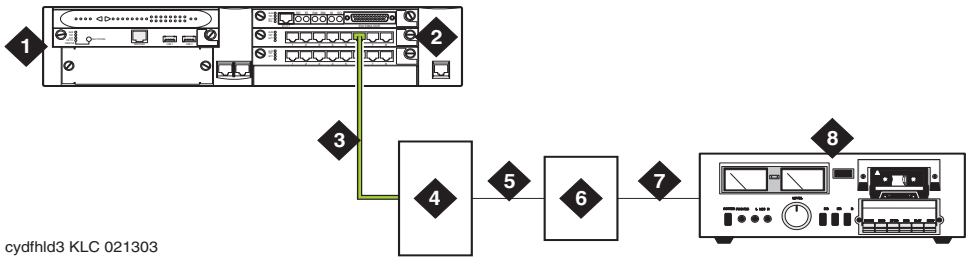


Figure notes:

1. **G700 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **KS-23395-L4 coupler**
5. **8-pair modular cord**
6. **909A/B universal coupler**
7. **8-pair modular cord**
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 42 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 42: Registered music-on-hold equipment connecting to KS-23395-L4 for a G700 Media Gateway

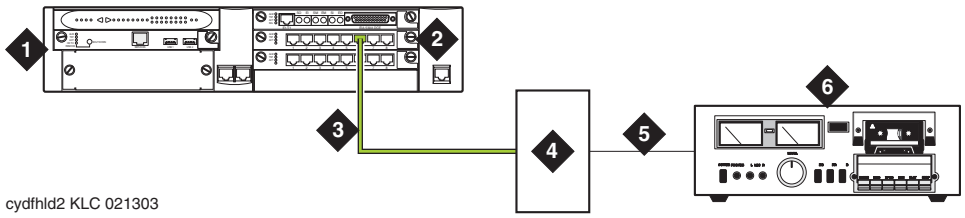


Figure notes:

1. **G700 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **KS-23395-L4 coupler**
5. **8-pair modular cord**
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 43 shows the connections for loudspeaker paging, dial dictation, or recorded announcement features on a G700 or G350 Media Gateway.

Figure 43: Typical loudspeaker equipment connections for a G700 or G350 Media Gateway

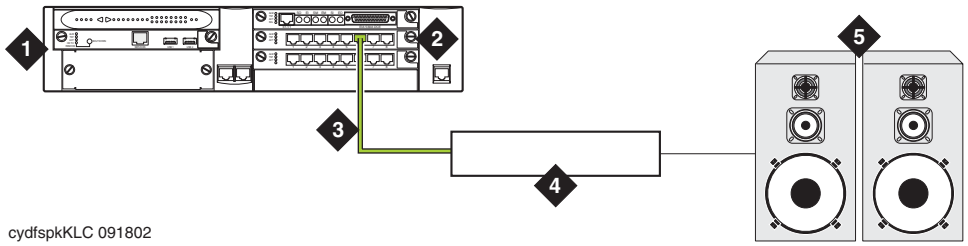


Figure notes:

1. **G700 or G350 Media Gateway**
2. **MM711 Analog Media Module**
3. **RJ-45 connection**
4. **Telephone hybrid (third party) device**
5. **Loudspeaker paging system**

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
- Converged Communications Server
- 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.

Converged Communications Server

For information on installing Avaya Converged Communications Server (CCS), see the *Converged Communications Server Installation and Administration Guide*, 555-245-705, and *SIP Support in Communication Manager R2.0*, 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 8: Telephones and adjunct systems.

This section is organized into the following chapters:

- Chapter 9: Manual installation of a new G700 with an S8300
- Chapter 10: Manual installation of a new G700 without an S8300
- Chapter 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware
- Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware
- Chapter 13: Manual upgrade of an existing G700 without an S8300

Note:

Automated procedures to perform many of these tasks, using Avaya wizard tools may be found in Section 2: G700 installation and upgrades - wizards.

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 28 to determine which task list is most appropriate for your upgrade or installation.

Table 28: Task lists for your manual upgrade or installation

	G700 with an S8300 (Primary or LSP)	G700 without an S8300	G700 Controlled by an S8300 with IA 770 INTUITY AUDIX Messaging
New Installation	Checklist 1 Chapter 2 Chapter 9	Checklist 2 Chapter 2 Chapter 10	See Installation Checklists in the IA 770 INTUITY AUDIX Messaging documentation, available on the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151
Upgrade an Existing System	S8300A to R3.0: Checklist 3 Chapter 11 S8300B to R3.0: Checklist 4 Chapter 12	Checklist 5 Chapter 13	

Checklist 1: Install a new G700 with an S8300 (Primary or LSP)

Use Checklist 1 to install a G700 Media Gateway with the following characteristics:

- The G700 has an S8300 Media Server configured as the primary controller

  or,

- The G700 has an S8300 Media Server configured as an LSP and is controlled by an S8300, S8500, or an S8700-series Media Server.

You will use Chapter 2: Hardware installation for the G700 Media Gateway and S8300 Media Server and Chapter 9: Manual installation of a new G700 with an S8300 with this checklist.

For help with connecting to and logging in to the G700 or S8300, see About connection methods on page 54.

Checklist 1: Manually install new G700 with an S8300 (Primary or LSP)

Major Tasks	Subtasks
Installation Overview on page 436	- G700 components - Software and firmware files - Access to the Server CD - Access to the S8300 and G700
Before Going to the Customer Site on page 439	- Install TFTP Server or Obtain USB CD Drive - Get planning forms - Get the G700 serial number - Check FTP server for backups - Obtain service pack files, if needed - If using IA770, obtain service pack and language files, if needed - If using IA770, obtain Ethernet interface IP address and Subnet mask - Complete the RFA process - Obtain static craft password
Hardware installation for the G700 Media Gateway and S8300 Media Server on page 75	- On site checklist - Unpack and check the order - Install the G700 - Cable multiple units - Attach ground conductors
Install the S8300 on page 446	- Insert the S8300 - Remaster the hard drive and install new software - Download service pack and security files - Verify time, date, and time zone - Install license and authentication files - Save translations - Install Communication Manager service pack, if any - Install IA770 service pack, if any
Configuring the S8300 on page 459	- Backup data - Set server identities - Configure Ethernet interfaces - Configure LSP - Configure Ethernet adjuncts - Configure External DNS server - Set Static network routes, if necessary - Configure network time server - Set modem interface - Update system - Load Key files, if necessary

Checklist 1: Manually install new G700 with an S8300 (Primary or LSP) (continued)

Major Tasks	Subtasks
If using IA770, install messaging software on page 475	- Log in to the S8300 platform - Stop the system - Auto-install the messaging software - Restart the system - Enable messaging on the S8300 Web interface
Configure the G700 Media Gateway on page 476	- Assign IP addresses to the G700 processors - Set up IP routing for the stack - Set up default IP route for the G700 - Check IP connections - Set up controller list for the G700 - Configure X330 Expansion Module, if necessary
Install New Firmware on the G700 on page 485	- Verify contents of the tftp directory - Determine which firmware to install - Install firmware on the P330 stack processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree
Administer Communication Manager on page 494	- Reboot the system - Assign node names, if necessary - Administer network regions - Assign LSPs to network regions - Administer IP interfaces - Administer the LSP form - Add media gateway - Verify changes - Enable announcements, if necessary - Save translations
Considerations for IP Phones Supported by a Local Survivable Processor on page 510	
Set Up SNMP Alarming on the G700 on page 511	
Complete the Installation of the S8300 (if the Primary Controller) on page 515	- Register the system - Back up the system - Check planning documentation - Connect and administer test endpoints - Complete electrical installation - Enable adjunct systems

Checklist 1: Manually install new G700 with an S8300 (Primary or LSP) (continued)

Major Tasks	Subtasks
If using IA770, administer Communication Manager for Integrated Messaging on page 516	
Complete the Installation Process (for an S8300 LSP) on page 517	- Check planning documentation - Connect and administer test endpoints - Complete electrical installation - Enable adjunct systems

3 of 3

Checklist 2: Install a new G700 without an S8300

Use Checklist 2 to install a G700 Media Gateway with the following characteristics:

- The G700 does not have an S8300 and is controlled by an external S8300, S8500, or S8700-series Media Server.

You will use Chapters 2 and 10 with this checklist.

For help with connecting to and logging in to the G700, see About connection methods on page 54.

Checklist 2: Manually install a new G700 without an S8300

Major Task	Subtasks
Before going to the customer site on page 523	- Get planning forms - Get the G700 serial number -- Set up TFTP server, if necessary - Download firmware files
Hardware installation for the G700 Media Gateway and S8300 Media Server on page 75	- On site checklist - Unpack and check the order - Install the G700 - Cable multiple units - Attach ground conductors

1 of 2

Checklist 2: Manually install a new G700 without an S8300 (continued)

Major Task	Subtasks
Configure the G700 on page 526	- Assign IP addresses to the G700 processors - Set up IP routing for the stack - Set up default IP route for the G700 - Check IP connections - Set up controller list for the G700 - Configure X330 Expansion Module, if necessary
Prepare to install firmware on the G700 on page 536	- Verify contents of the tftp directory - Determine which firmware to install
Install New Firmware on the G700 Media Gateway on page 539	- Install firmware on the P330 stack processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree
Administer Communication Manager on page 544	- Reboot the system - Assign node names, if necessary - Administer network regions - Assign LSPs to network regions - Administer IP interfaces - Administer the LSP form - Add media gateway - Verify changes - Enable announcements, if necessary - Save translations
Complete the Installation Process on page 561	- Check planning documentation - Connect and administer test endpoints - Complete electrical installation - Enable adjunct systems

2 of 2

Checklist 3 Upgrade an existing G700 with an S8300A to R3.0

Important:
You must replace the S8300A with an S8300B for this upgrade.

Use Checklist 3 to upgrade a G700 Media Gateway with the following characteristics:

- The G700 has an S8300A Media Server configured as the primary controller.

  or,

- The G700 has an S8300A Media Server configured as an LSP and is controlled by either an S8300, S8500, or S8700-series Media Server.

You will use Chapter 11 with this checklist. For help with connecting to and logging in to the G700 or S8300, see About connection methods on page 54.

Checklist 3: Task list to manually upgrade an existing G700 with an S8300A (R1.x or R2.x to R3.0)

Major Tasks	Subtasks
Before going to the customer site on page 566	- Install TFTP server or obtain USB CD drive - Fill in EPW (if upgrading from 1.1) - Get planning form - Get the G700 serial number - Check number of allocated ports - Check FTP server for back up - Get software/firmware files - Download Communication Manager service pack and IA770 service pack software to laptop, if necessary - Complete the RFA process - Obtain static craft password
Preparing for the upgrade to R3.0 on-site on page 576	- Check current software release - Pre-Upgrade tasks — If the Target S8300 is the Primary Controller - Get IA770 data and stop IA770 - Back up system files - Record configuration information

1 of 2

Checklist 3: Task list to manually upgrade an existing G700 with an S8300A (R1.x or R2.x to R3.0) (continued)

Major Tasks	Subtasks
Upgrading the S8300A on page 589	- Install the pre-upgrade service pack - Linux Migration Backup - Replace the S8300A - Remaster and Upgrade the S8300: - Verify software version - Copy licence and authentication files to the S8300 - Disable messaging - Configure S8300 network parameters - Verify connectivity to backup server - Restore backup data - Verify date and time - Install post-upgrade service pack, if necessary - Verify S8300 configuration - Install license file, if necessary - Install authentication file, if necessary - Save translations (if not using IA770) - Verify operation
Upgrade the firmware on the G700 Media Gateway on page 619	- Verify contents of the tftp directory - Determine which firmware to install - Install firmware on the P330 stack processor -Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any - Set Rapid Spanning Tree If using IA770: - Install and restart IA770 - Save translations - Install IA770 service pack, if any - Install optional language files, if any
Complete the upgrade process (S8300 is the primary controller) on page 636	- Check media modules - Enable scheduled maintenance - Busyout trunks - Check for translation corruption - Resolve alarms - Re-enable alarm origination - Back up system - Restart LSPs, if any

2 of 2

Checklist 4 Upgrade an existing G700 with an S8300B to R3.0

Use Checklist 4 to upgrade a G700 Media Gateway with the following characteristics:

- The G700 has an S8300B Media Server configured as the primary controller.

  or,

- The G700 has an S8300B Media Server configured as an LSP and is controlled by either an S8300, S8500, or S8700-series Media Server.

You will use Chapter 12 with this checklist. For help with connecting to and logging in to the G700 or S8300, see About connection methods on page 54.

Checklist 4: Task list to manually upgrade an existing G700 with an S8300B (R2.0.x to R2.2.x)

Major Tasks	Subtasks
Before going to the customer site on page 640	- Get planning form - Get the G700 serial number - Check number of allocated ports - Check FTP server for back up - Get software/firmware files - If using IA770, obtain service pack and language files, if any - Complete the RFA process - Obtain static craft password - Download service pack software to laptop, if necessary
On-site Preparation for the Upgrade on page 648	- Pre-Upgrade tasks — If the Target S8300 is the Primary Controller - Get IA770 data and stop IA770 - Back up recover system files - Install new license and authentication files, if necessary - Save translations, if new license and/or authentication files installed - Transfer files from CD or laptop
Upgrade the S8300 on page 666	Install the Upgrade Software: - Upgrade S8300 - Make the upgrade permanent - Install Communication Manager service pack, if any - Install IA770 service pack, if any

1 of 2

Checklist 4: Task list to manually upgrade an existing G700 with an S8300B (R2.0.x to R2.2.x) (continued)

Major Tasks	Subtasks
Upgrade the G700 Firmware on page 674	- Verify contents of the tftp directory - Determine which firmware to install - Install firmware on the P330 stack processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree
Installing IA770 service pack (or RFU) files, if any on page 683	- Download the service pack software - View the service pack documentation
Completing the upgrade process (S8300 is the primary controller) on page 684	- Check media modules - Enable scheduled maintenance - Busy out trunks - Check for translation corruption - Resolve alarms - Re-enable alarm origination - Back up system - Restart LSPs, if any

2 of 2

Checklist 5: Upgrade an existing G700 without an S8300

Use Checklist 5 to upgrade a G700 Media Gateway with the following characteristics:

- The G700 does not have an S8300 and is controlled by an external S8300, S8500, or S8700-series Media Server.

You will use Chapter 13 with this checklist. For help with connecting to and logging in to the G700, see About connection methods on page 54.

Checklist 5: Task list to manually upgrade an existing G700 without an S8300

Major Tasks	Subtasks
Before going to the customer site on page 689	- Get planning forms - Get the G700 serial number - Set up TFTP server, if necessary - Download firmware files
On-site preparation for the upgrade on page 692	- Verify contents of the tftp directory - Determine which firmware to install
Install new firmware on the G700 Media Gateway on page 695	- Install firmware on the P330 stack processor - Install firmware on the G700 media gateway processor - Install firmware on the media modules - Install firmware on other G700s in the stack or network, if any -Set Rapid Spanning Tree

Chapter 9: 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 S8300B 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*** Communication Manager software installed on the hard drive. The hard drive contains only the remastering program (RP) software, which remasters the hard drive and installs the Communication Manager Software from the Server CD. To install the software, you need to have the Avaya TFTP Server installed on your laptop or use an external USB CD-ROM drive.

However, the S8300B may occasionally ship with Communication Manager software installed. In this case you must use an external USB CD-ROM drive — you cannot use the TFTP server on the laptop. See About access to the Server CD on page 436 for more information.

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.

Important:

This installation procedure requires that TFTP server software is installed on the technician's laptop. If the TFTP server is not installed on the laptop, you can use an external USB CD-ROM drive instead.

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

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 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 G700 components

A P330 stack processor is built into the G700 Media Gateway. (This processor is also known as the *Layer 2 switching processor*). The G700 also contains an MGP processor, a VoIP processor, and media modules. Updating the firmware for one or more of these processors and/or media modules is a required part of most S8300 software upgrades.

About software and firmware files

A new S8300 Media Server should have only the remaster program (RP) software installed on its 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.

The file containing the S8300 software and G700 firmware has a *.tar extension. The *.tar file is on the “Unity” 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 Server CD

The R3.0 Communication Manager software and other files needed for the R3.0 upgrade are on the Server CD that you take to the customer site.

You can make the Server CD available to the upgrade process in one of two ways:

- ***Recommended:*** Place the CD in the CD-ROM drive on the technician’s laptop. This method requires that the Avaya TFTP Server software (available at support.avaya.com) is installed on the technician’s laptop. This method requires that the S8300B ***does not*** have Communication Manager software installed on its hard drive.

  or,

- Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate. This method works whether or not Communication Manager software is installed on the S8300B hard drive.

Important:

Before you go the site, you must either have the TFTP server installed on your laptop (recommended) or have an external USB CD-ROM drive.

The new S8300B will normally not have Communication Manager software installed on its hard drive. You should check the S8300B that you will be installing (or ask the customer to check) before going to the site to determine whether you need to have the external USB CD-ROM drive. If software is not installed, the label on the hard drive will say “S8300B Hard Drive Without CM Software.” If software is installed, the label will indicate the software release. If software is installed, you must use the external USB CD-ROM drive because the TFTP server on your laptop will not work.

This chapter describes the upgrade procedure with the TFTP Server software installed on the laptop and using the laptop CD-ROM drive as source of the upgrade software. For instructions on obtaining and installing the Avaya TFTP Server, see Appendix D: Install the Avaya TFTP server

System Access

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.

How is normal access to the S8300 and G700 provided

You can access the S8300 and G700 in several ways with either a direct connection or LAN connection.

Note:

Before the Upgrade Tool can be used to upgrade software on an LSP or firmware on a G700, as summarized below, the LSP must be administered on the primary controller.

Connecting directly to a target S8300

If you are at the location of the target S8300 (primary or LSP), you can connect directly to the S8300 Services port.

To install or upgrade directly

1. Install the S8300 software by:
   - Opening the Web interface and using the Avaya Installation Wizard

     or,
   - Opening the Web interface and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or the Upgrade Tool

     or,
   - Opening a telnet session to the S8300, and then telnet to the P330 stack processor

Connecting directly to the remote primary server (S8300, S8500, or S8700)

In this case, the target S8300 is an LSP. If you are at the location of the remote primary server, you can connect directly to the remote server's Services port.

To install or upgrade the target LSP remotely

1. Install the S8300 (LSP) software by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool

     or,
   - Opening a telnet session to the primary server and then telnet to the P330 stack processor and perform the installation commands

Note:

For direct connections, the TFTP server must be on the Customer LAN, not on your laptop.

Connecting using the customer's LAN

If you can connect to the customer's LAN, you can:

1. Install the S8300 software by:
   - Opening the Web interface on the S8300 and using the Avaya Installation Wizard

     or,

   - Opening the Web interface on the S8300 and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface on the primary server and using the Avaya Installation Wizard or Upgrade Tool

     or,

   - Opening a telnet session to the P330 stack processor and perform the installation commands

Note:

For LAN connections, the TFTP server can be your laptop or a customer computer on the LAN.

See About connection and login methods on page 47 for details on how physically to connect and log into the G700.

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.

Perform the following pre-installation tasks:

Upgrading to release 3.0 (Install TFTP server or obtain USB CD-ROM drive)

Collecting Upgrade Information

Obtaining service pack files, if needed

If using IA770, obtaining service pack and language files

Completing the RFA process (Obtaining license and password file)

Upgrading to release 3.0 (Install TFTP server or obtain USB CD-ROM drive)

Upgrading Communication Manager on an S8300 to release 3.0 requires remastering the S8300B hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on:

- Your laptop if a TFTP server is installed

  or,

- An external USB CD-ROM drive

You must have the Avaya TFTP server software installed on your laptop or take a USB CD-ROM drive to the site. If you do not already have the Avaya TFTP server installed on your laptop, you can obtain the software from the Avaya Support website and install it as described in Appendix D: Install the Avaya TFTP server.

Important:

If the new S8300B that you will be installing has Communication Manager software installed on its hard drive, you must use an external USB CD-ROM drive instead of the TFTP server on your laptop. See About access to the Server CD on page 436.

Collecting Upgrade Information

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.

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 the FTP Server for Backing up Data

During the installation and upgrade procedures, you will need to back up the system data to an FTP server. Normally, you will use an FTP server on the customer's LAN for backups.

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

Check with your project manager or the customer for this information.

Important:
Before going to the customer site, make sure that you can use a customer server for backups.

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

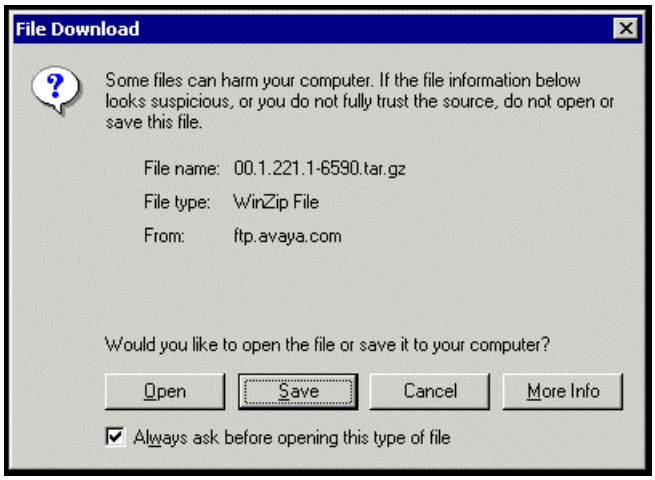
1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access http://www.avaya.com/support on the Internet to copy the required Communication Manager service pack file to the laptop.

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 3.0**).
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.

If using IA770, obtaining service pack and language files

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

1. On the Avaya Support website, double click on **Messaging** in the list on the left.
2. Scroll down to the INTUITY links and double click on **IA 770 INTUITY AUDIX Messaging Application**.
3. Double click on **All Documents**.
4. 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**.
5. Double click on the file name. For example, **C6039rf+c.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 will download the appropriate language files from a language CD. The customer should have the language CDs at the site. If not, you need to obtain the appropriate language CDs and take them to the site.

If using IA770, obtain 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 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, S8500, S8700, S8710, or Blade 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.

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. When inserting the S8300 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.

2. The LED panel (above slot V1) must be inserted together with the S8300 circuit pack.

   a. 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).

   b. 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.

3. Secure the S8300 faceplate with the thumb screws.

   Tighten the thumb screws with a screw driver.

4. Power up the G700 by plugging in the power cord.

5. Connect the laptop to the Services port on the faceplate of the S8300.

Installing Communication Manager Software

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 S8300B 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.
5. Insert the Unity CD in the CD-ROM drive:
   - If TFTP server software is installed on your laptop, ***start the TFTP server program*** (TFTPServer32.exe), and insert the Communication Manager unity CD in the laptop's CD drive.

CAUTION:

Verify good AC power connections to the laptop. Do not attempt a remastering using only the laptop's battery power.

Note:

Shut down all applications on the laptop except for the TFTP server and the telnet client. Other background applications can overly use laptop resources.

Note:

Ensure that the **Outbound file** path is set to the root of your laptop's CD-ROM drive. (For example, D:\)

To check:

i. Open the **System** menu in the TFTP server program

ii. Select **Setup**

iii. Open the **Outbound** tab.

iv. To change the **Outbound file** path, click the **Browser** button and select the **CD** drive.

or,

- If your laptop does not have TFTP server software installed, attach an external USB CD-ROM drive to one of the USB ports on the S8300B and insert the Unity CD in the drive.

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.

NOTE: If you get the login prompt instead of the RP screen

If the telnet login prompt appears instead of the RP screen, the hard drive contains a Communication Manager software release. In this case, if you have a USB CD-ROM drive, connect the drive to a USB port on the S8300 and insert the unity CD. Then log in to the telnet session (using the initial *craft* login) and use the **Shutdown Server** feature on the Maintenance Web Interface to reboot the system. After the reboot completes, telnet to 192.11.13.6 and the RP screen should now be displayed.

If you do not have the USB CD-ROM, you cannot proceed with the upgrade procedure described in this chapter. However, you can upgrade the Communication Manger software using the procedure described in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware and then return to this chapter.

To upgrade using the procedure in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware

1. Complete the procedures starting at Installing the pre-upgrade software service pack on page 658 and ending with Making the upgrade permanent on page 670. Note that you must have a copy of the license and authentication files on your laptop and install them before doing the upgrade.
2. Return to this chapter and complete the procedures starting with Verifying software version on page 251, using the initial *craft* login.
3. Complete all the remaining procedures ***except*** installation of the license and authentication files, which was done in step 1.

Alternatively, you can obtain a USB CD-ROM drive or an S8300B with only the RP software and proceed from Remastering the hard drive and installing the upgrade software on page 245.

The first RP screen

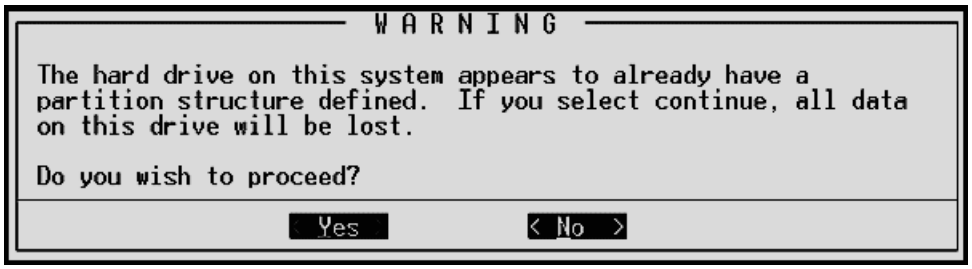
Tip:

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.

4. Select **Install** and press **Enter**.

   If a **Warning** screen appears,

RP Warning screen

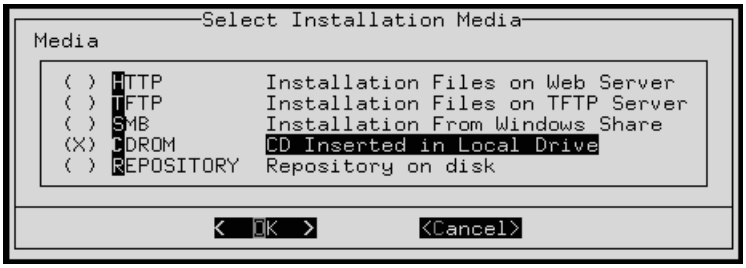


select **Yes** and press **Enter**.

Note:

At this point, the installation script looks for the Unity CD either on your laptop or in a CD drive connected to the USB port. If you do not have the TFTP server running on the laptop, and a CD drive is not attached to a USB port, you will see the **Select Installation Media** screen:

The Select Installation Media screen



If you see the Select Installation Media screen:

a. Start up the TFTP server on your laptop, or connect a USB CD-ROM drive to one of the USB ports.

b. Insert the unity CD in the laptop or USB drive.

c. Select either **TFTP** or **CDROM**.

d. Select **OK,** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen

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

6. The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen

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

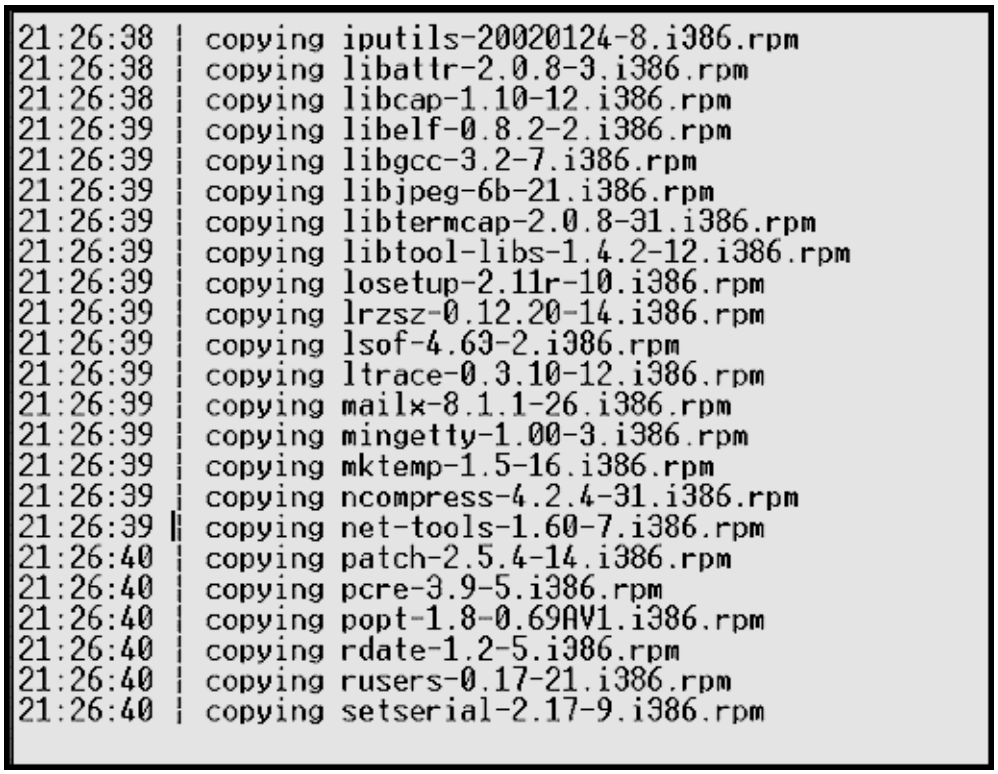
   At this point, the following processes are initiated:

   a. The S8300 hard drive is 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



These processes take 15–30 minutes. When the media server is ready to reboot, the following screen flashes for about 5 seconds.

Software and firmware update reminder

When the installation is complete, the CD drive door opens and the system reboots automatically. The reboot takes 1–3 minutes.

In the event you used the laptop TFTP server and you have a problem with power and the S8300 does not reboot, there are two methods of recovery:

- Use the USB CD-ROM to plug into the S8300 and repeat the remastering process using the Unity CD.
- Arrange access to another hard drive (comcode 700307028) should it be necessary to perform the TFTP remaster procedure on it.

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 on to Integrated Management and launch the Maintenance Web Interface.
2. Under Server, click **Software Version**.
3. Verify that the media server is running Release 3.0 software.

   The **Report as:** string should show **R012x.01** at the beginning of the string. For example, **R012x.01.0.411.1**.

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. For release 2.0 and later, this *pub* directory will be used in place of the */var/home/ftp* directory that was used in previous releases.

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

To copy files to the S8300 hard drive

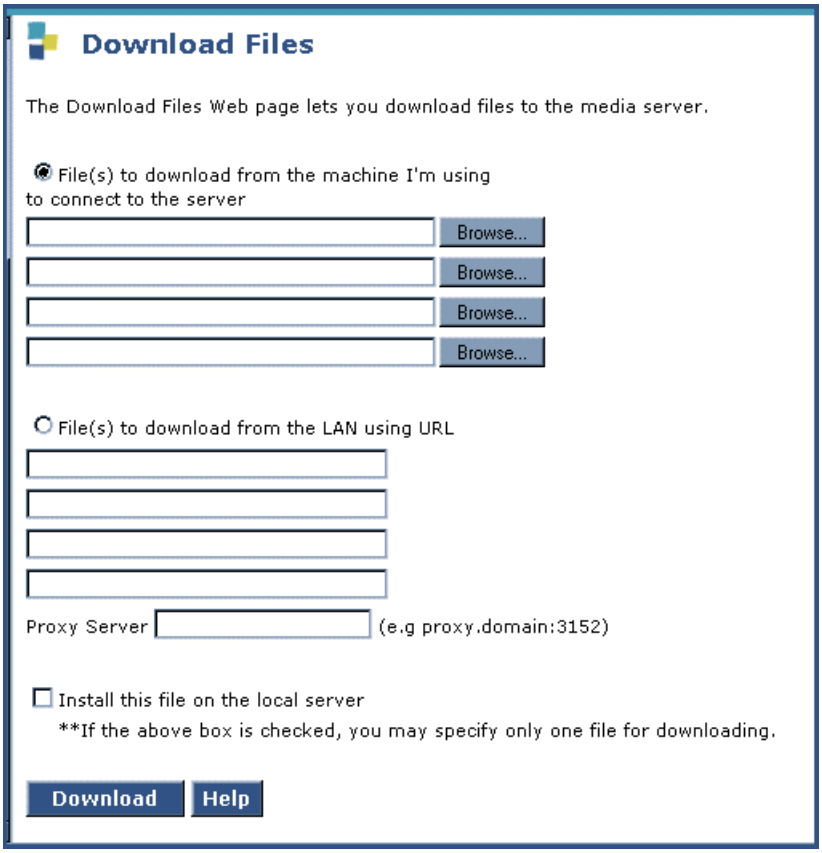
1. Log on to Integrated Management and launch the Maintenance Web Interface.

   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.)

2. Under Miscellaneous click **Download Files**.

Download Files screen



3. 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`**.

4. 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:

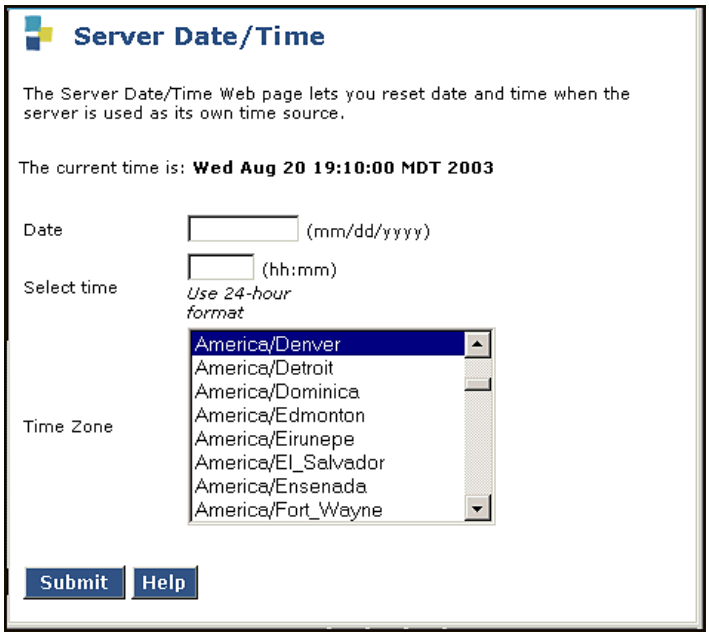
   Remove the Server CD from the CD drive.

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).

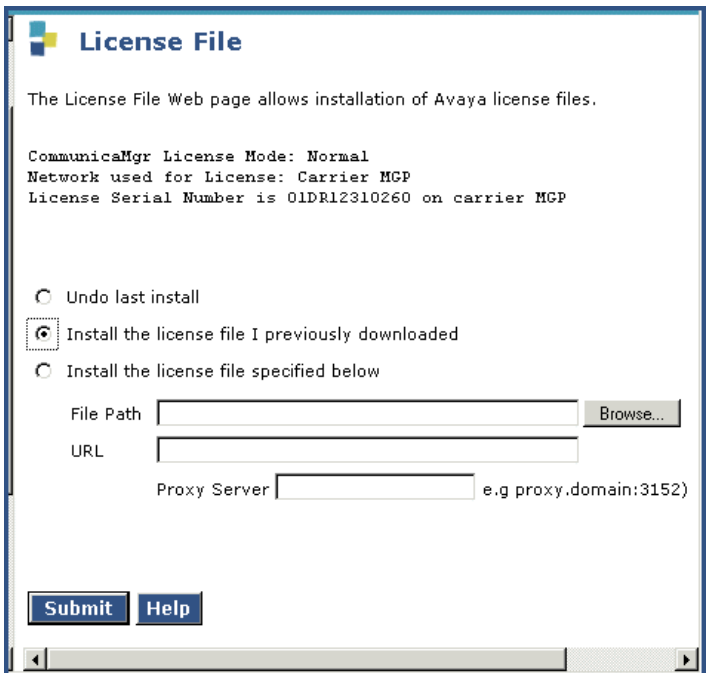
Installing License and Authentication Files

To install license and authentication files

1. Under Security, select **License File**.

   The **License File** screen displays.

License File Screen



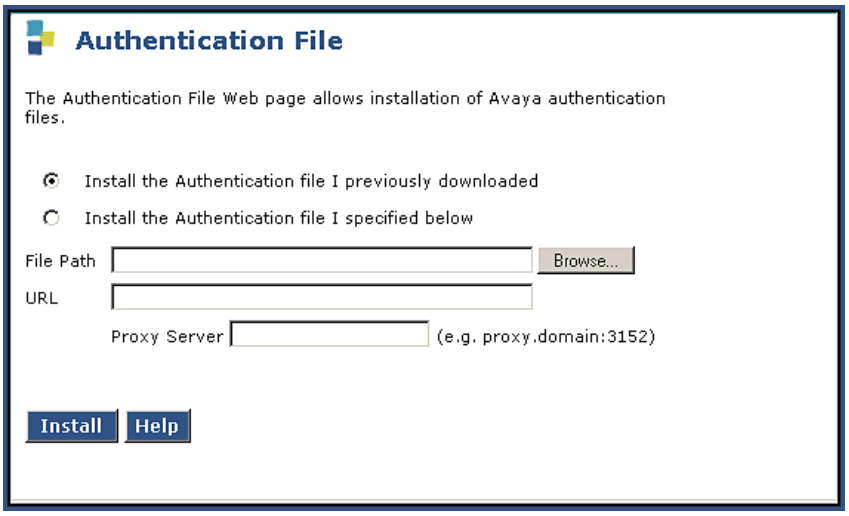
2. Select "Install the license file I previously downloaded" and click **Submit**.

   The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.

   The **Authentication File** screen displays.

Install Authentication Screen



4. Select "Install the Authentication file I previously downloaded" and click **Install**.

   The system tells you the authentication is installed successfully

Saving Translations

Note:

Skip this procedure if the S8300 is an LSP.

To save translations

1. In a telnet session, open a SAT session, and log in again as *craft* (or *dadmin*).
2. At the SAT prompt, type **`save translation`** and press **Enter**.

   When the save is finished, the system displays the message:

   Command successfully completed

Installing Communication Manager service pack files, if any

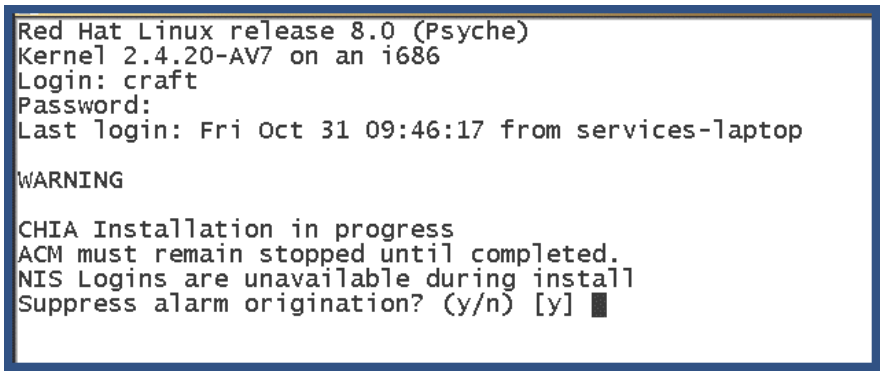
Note:

Skip this procedure if there are no Communication Manager update files to install.

To install Communication Manager update files

1. From your laptop, open a telnet session to the S8300.

   If IA770 will be used with this system, the IA770 software is automatically installed after the Communication Manager software is installed. If the IA770 installation has not completed, the following warning screen will appear.



CAUTION:

If this warning screen appears, close the telnet session, wait about 5 minutes, and try again.

2. At the telnet prompt, type **`cd /var/home/ftp/pub`** 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 update .tar.gz file you have uploaded, if any.

5. Type **update_unpack *<update>* .tar.gz**, and press **Enter**,

   where ***<update>*** is the release or issue number of the latest update file (for example, **00.0.218.4-1003.tar.gz**).

6. Type **update_show** again and press **Enter** to list Communication Manager files.

   Verify the new software file was installed.

7. Type **update_activate *<update>***, and press **Enter,**

   where ***<update>*** is the release or issue number of the latest update file (for example, **00.0.218.4-1003**). Do *not* use the .tar.gz extension at the end of the file name.

   The S8300 goes through a software **reset system 4**. The S8300 also may display the message:

   ```
   /opt/ecs/sbin/drestart 1 4 command failed
   ```

   Ignore this message. You must wait until the restart/reset has completed before entering additional commands.

   The S8300 displays a message that the update was applied.

8. Type **update_show** again and press **Enter** to list Communication Manager files.

   Verify the new software file was applied.

Configuring the S8300

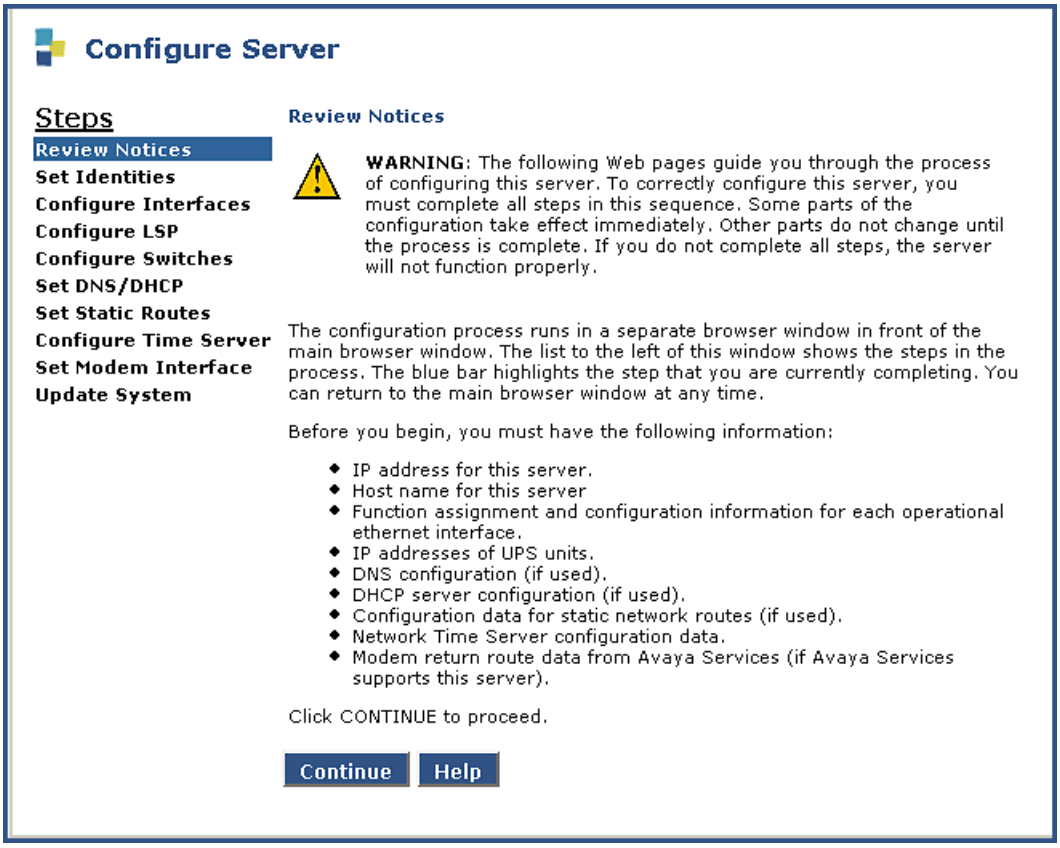
To configure the S8300 server using the Maintenance Web Interface

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



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 on page 515.

3. Click **Continue**.

   The **Select Method** screen appears.

Select Method Screen

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:

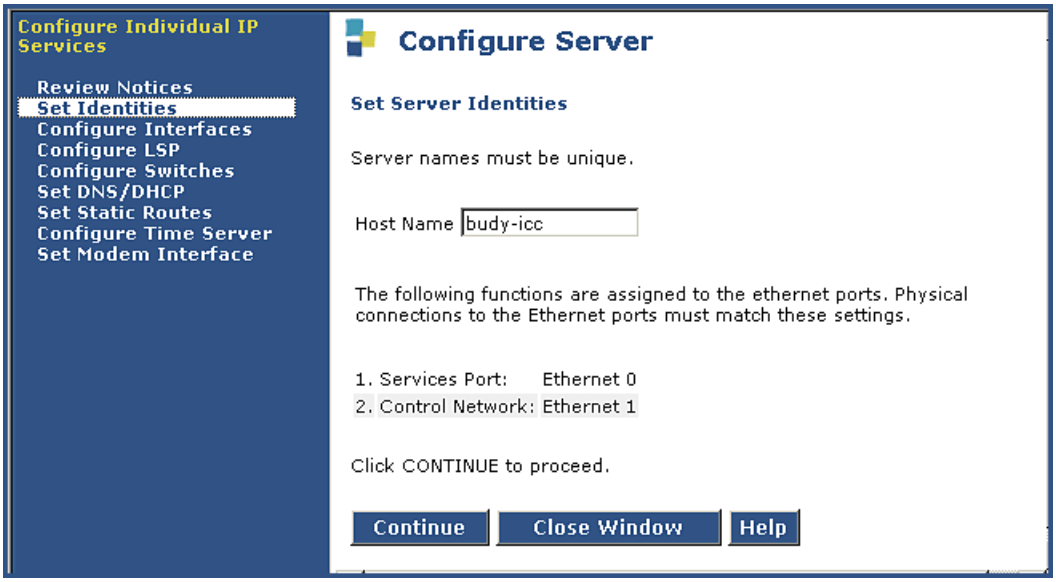
   This option is for the built-in Web Interface configuration wizard, *not* the Avaya Installation Wizard (IW).

   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 Server Identities** screen appears.

Set Server Identities Screen



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.

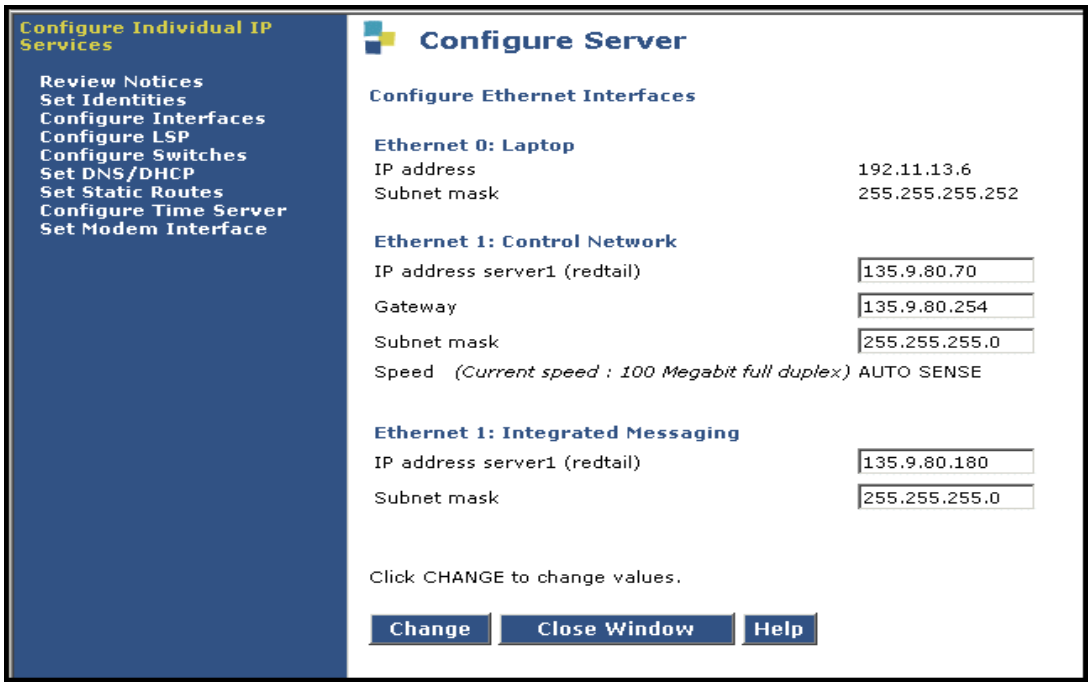
   Note:

   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



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.
   - **Ethernet 1: Integrated Messaging**
     - **IP Address server1 (*hostname*)** assigned to Integrated Messaging. Check your planning forms.
     - **Subnet mask** with the *same* value as the subnet mask of the hosting media server.

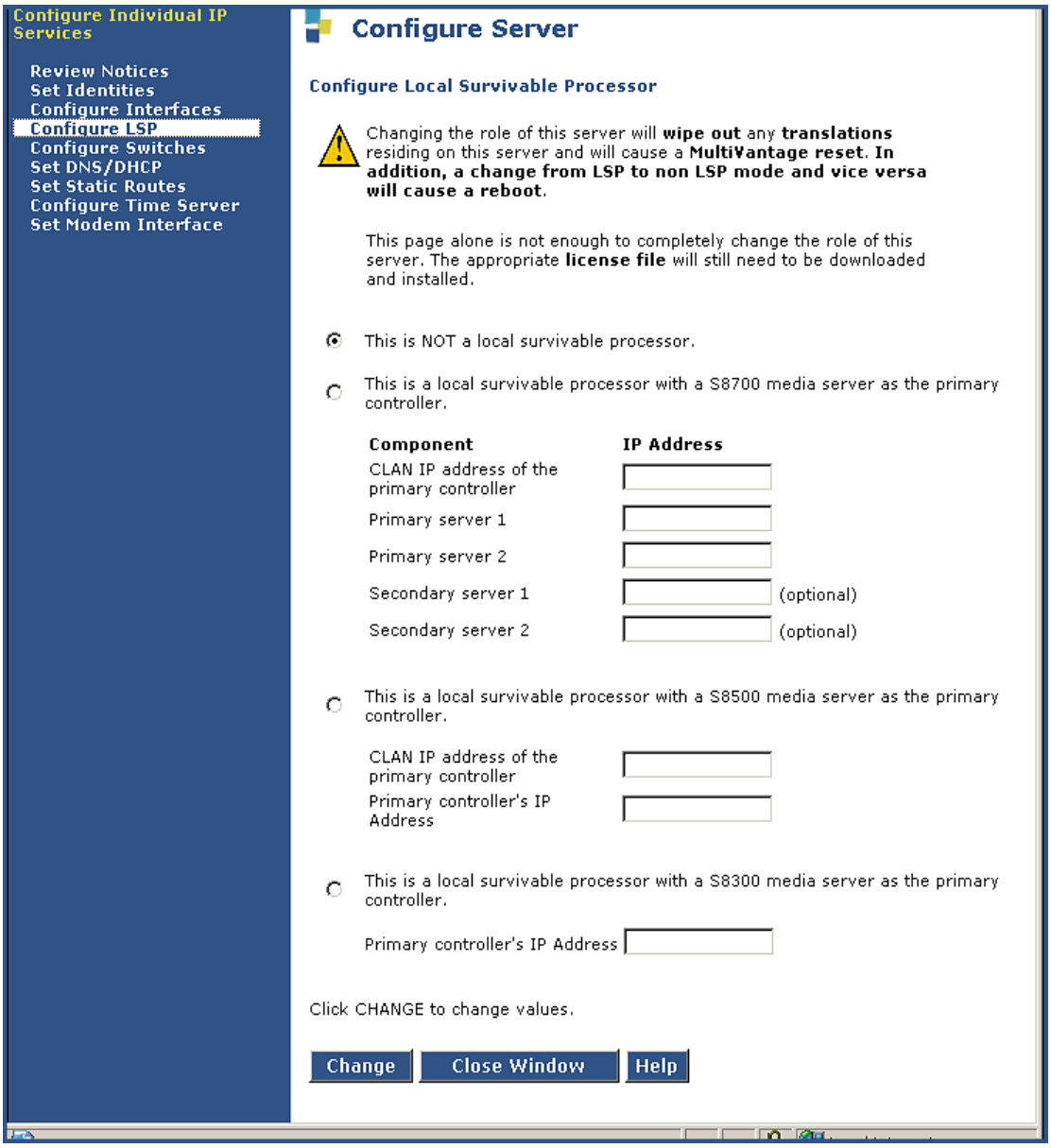
   CAUTION:

   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



10. Select one of the following options:
    - This is NOT a local survivable processor.
    - This is a local survivable processor (LSP) with an S8700-series media server as the primary controller.
    - This is a local survivable processor (LSP) with an S8500 media server as the primary controller.
    - This is a local survivable processor with a S8300 media server as the primary controller.

11. If you clicked the LSP option with an S8500 or S8700-series, complete the additional fields as follows:

    CLAN IP address of the primary controller — the IP address of any CLAN board in the S8700-series media server configuration.

    IP address of server 1 (required) — the IP address of the primary S8700-series server.

    IP address of server 2 (optional) — the IP address of the duplicated primary S8700-series server. If server 2 is present, this specific IP address must also be entered.

    IP address of secondary server 1 (optional) — the IP address of the secondary S8700-series server.

    IP address of secondary server 2 (optional) — the IP address of the duplicated secondary S8700-series server

    Note:

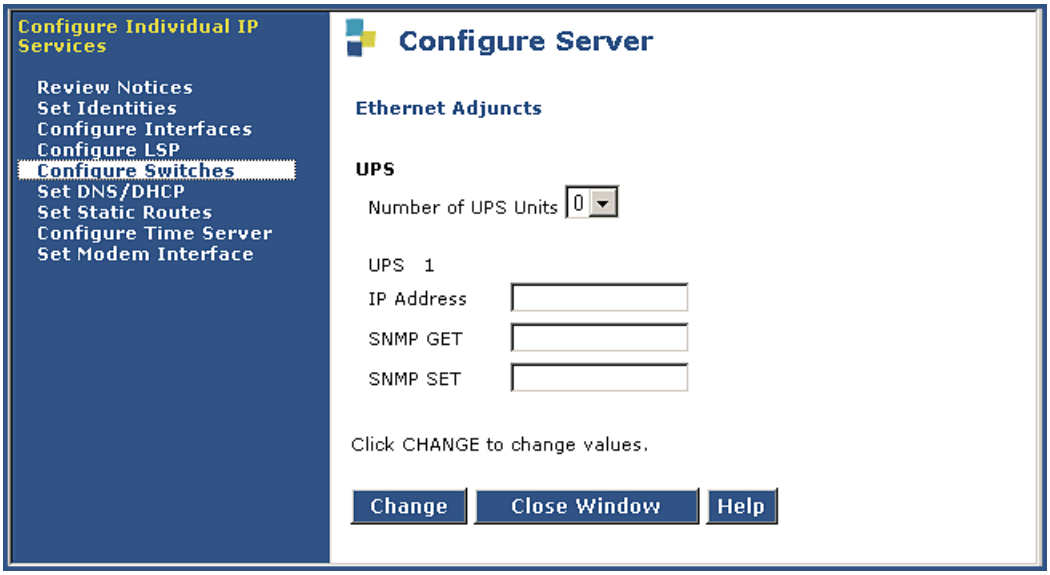
    The CLAN boards must be TN799DP running version 5 or greater firmware. Be sure to check the firmware version for these boards on the S8500 or S8700-series. For information on how to upgrade the firmware on the S8500 or S8700-series, please see the section "Upgrade Firmware in Selected Port Cabinet Packs" in *Upgrading the Avaya Media Server Configuration* in the S8700-series documentation portion of the *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

12. If you clicked the LSP option with an S8300, 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**.

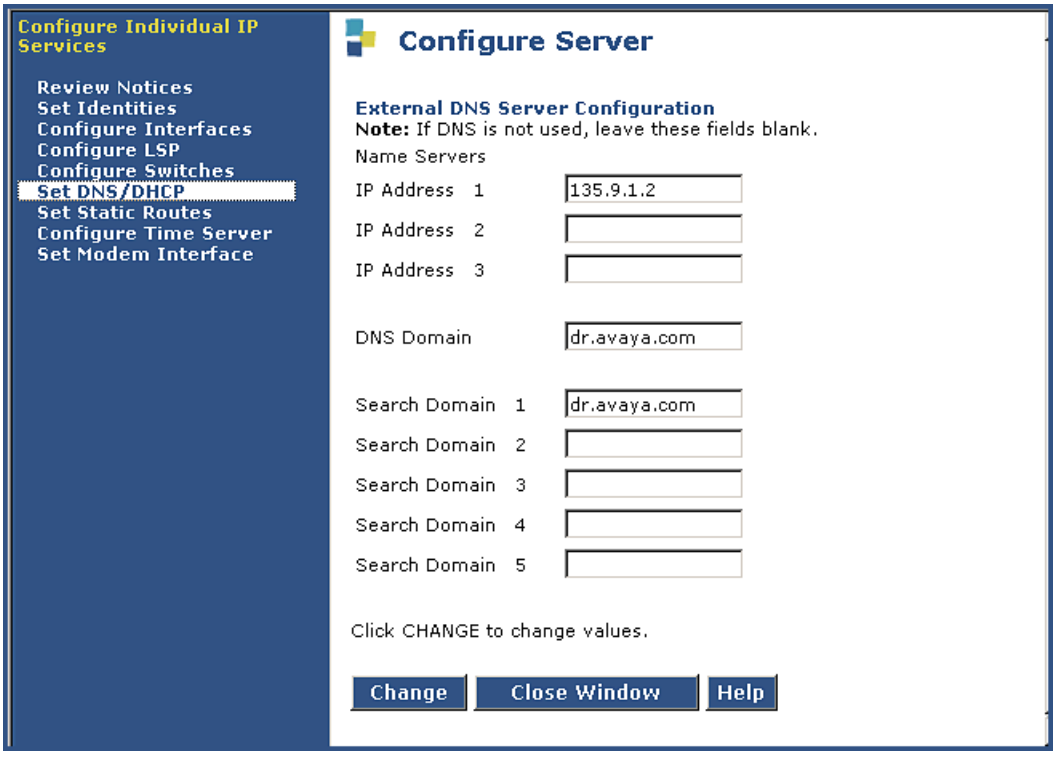
    The **External DNS Server Configuration** screen appears.

    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



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:

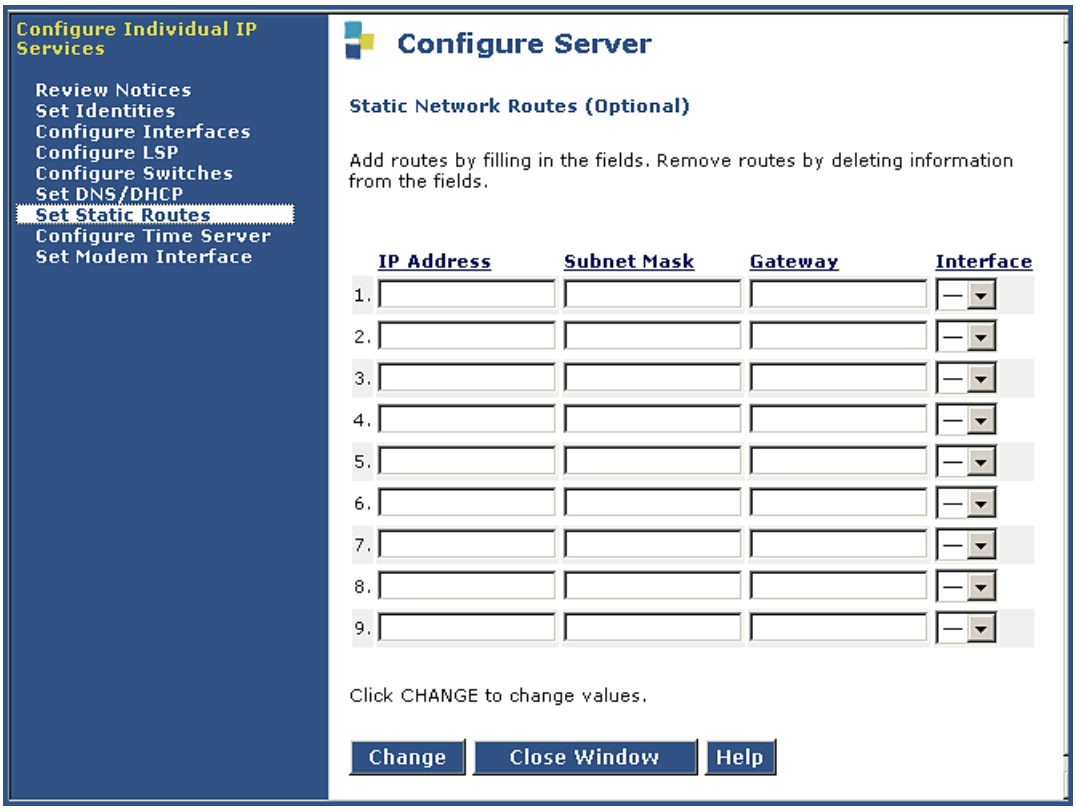
    For **Search Domain 1**, enter the *same domain name* you entered in the **DNS Domain** field above.

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

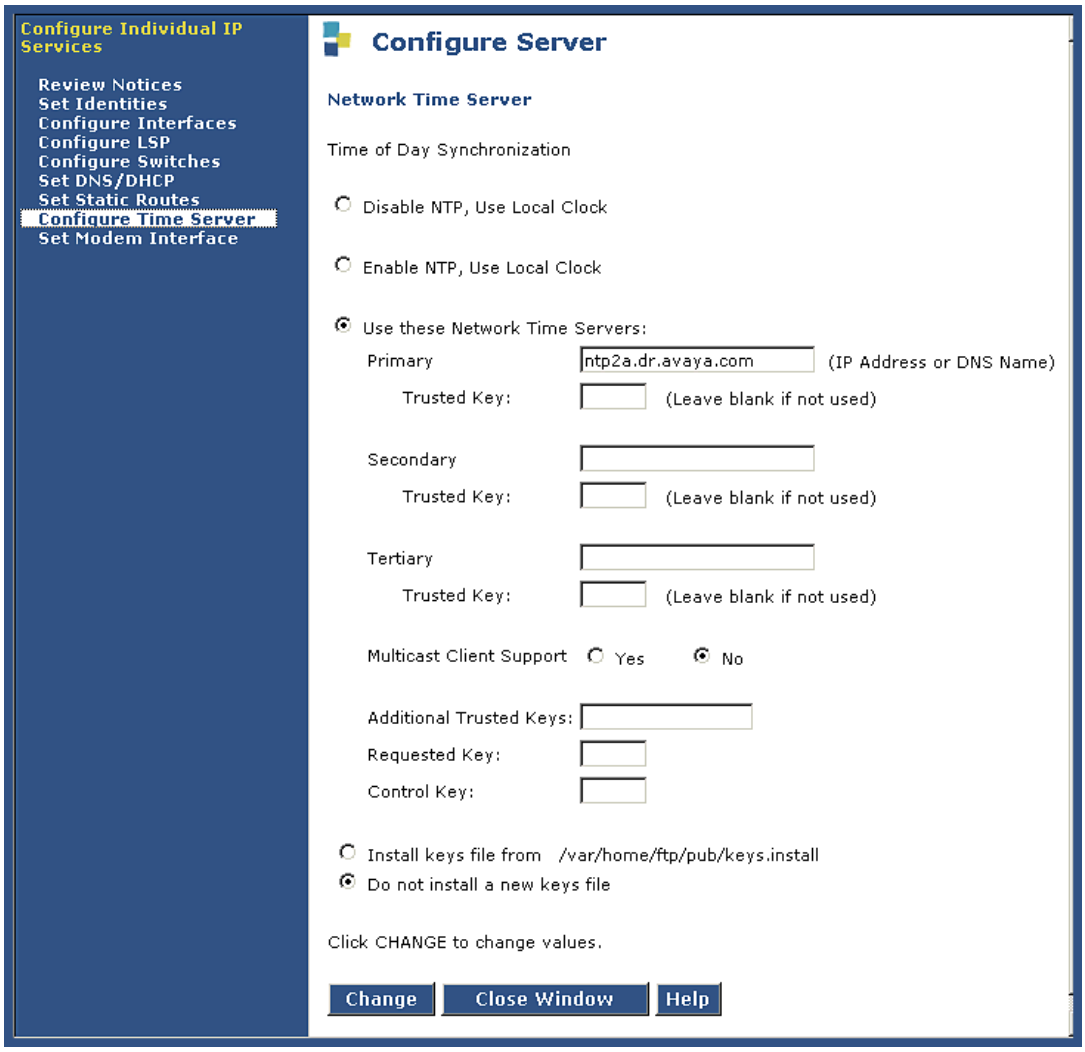


20. Click **Continue**.

    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



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**.

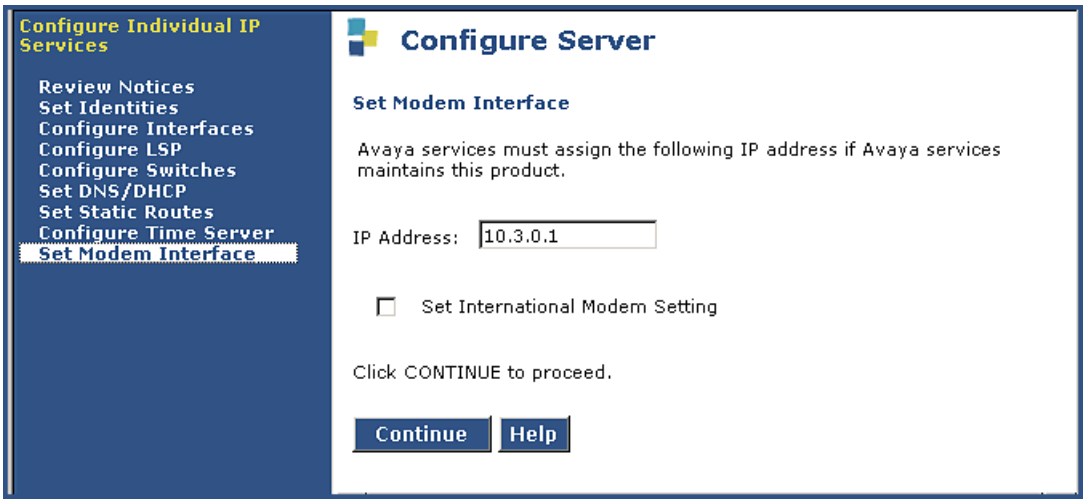
    Note:

    If you have a *keys.install file*, upload or create it now, if possible. See Providing the keys.install File (If Necessary) on page 473. 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



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 445.

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.

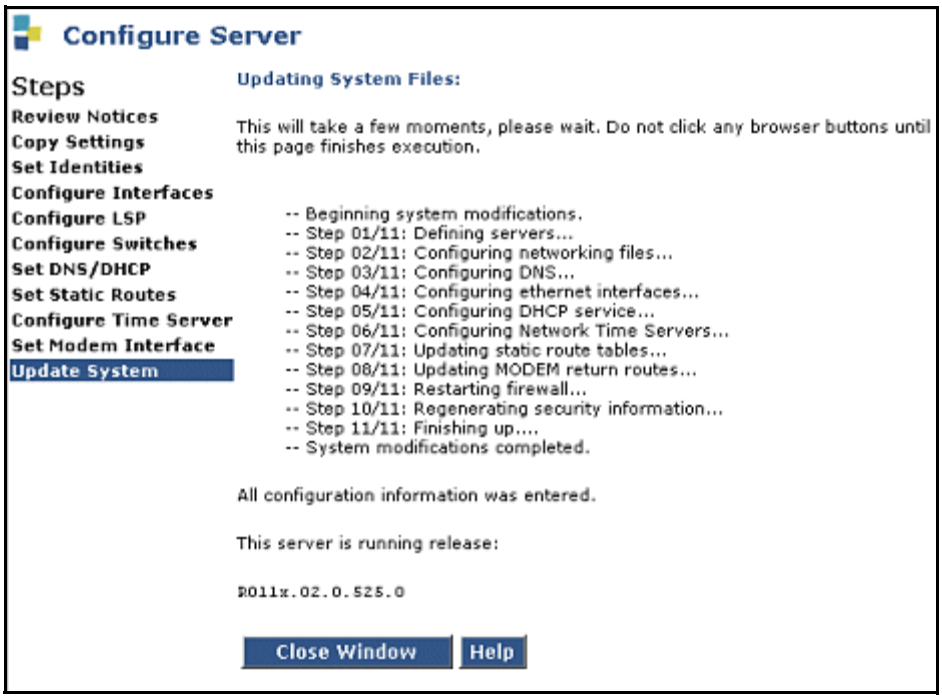
    If you don't do this, information in the wizard may not be processed correctly.

    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.

Setting the media server's time

To set the media server's time

1. In the main menu under Server, click **Set Server Time / Timezone**.

   The S8300 displays the **Set Server Time/Timezone** window.

2. 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).

3. When finished, click on the **Configure Server** window to continue.

   After NTP is enabled, time changes greater than 15 minutes will disrupt the synchronization with the NTS and NTP will shut down. You need to set the server's clock now so that synchronization can take place.

4. When finished, click **Continue**.

If using IA770, install messaging software

If you are using IA770 Integrated Messaging, you must install the messaging software at this time.

The tasks to accomplish this are:

1. Log in to the S8300 Media Server command line.
2. Stop the system.
3. Auto-install the IA770 messaging software.
4. Restart the system.
5. Enable messaging on the S8300 Media Server Web interface.

For detailed information on performing these tasks, refer to *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532.

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 **`nvram init`** to recondition the 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 21.25.0

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      : 00
HW Suffix       : A
FW Vintage      : 21.25.0

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 recondition the 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. Log in again at the **Welcome to P330** menu.
10. At the **P330-1(configure)#** prompt, type **`session mgp`**.

11. At the **MG-???-1(super)#** prompt, type **`configure`** to reach the configuration level of the command line interface.
12. 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

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>`*** is the IP address of the primary controller for this G700. If the primary controller is an S8700, this is the IP address of a C-LAN board that is connected to a pair of duplicated S8700/S8710s. If the primary controller is an S8300, this is 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 an S8700/S8710 duplicated pair or an S8300 configured as an LSP, depending on the G700's primary controller.

   CAUTION:

   If you need to change the mgc list, you must run **`clear mgc list`** before running **`set mgc list`** again.

   Table 29 describes the possible optional controllers for an S8300 and S8700/S8710 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.
S8500 or S8700 or S8710	**First:** IP address of the C-LAN for the S8500 or S8700/S8710 primary controller. **Next three:** one, two, or three IP addresses of alternate C-LANs and/or LSPs.

Note:

For an S8500 or S8700/S8710 primary controller, the last three IP addresses in the list can be either the addresses of C-LANS (which are connected to the same S8500 or pair of S8700/S8710s that act as primary controllers) or addresses of LSPs. If you enter a combination of both, you must list C-LANs first and the LSPs last, *after* the C-LANs.

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 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

Installing IA770 service pack files, if any

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   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.

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

```
FLASH MEMORY    IMAGE VERSION
Bank A          109
Bank B          210

ACTIVE NOW      ACTIVE AFTER REBOOT
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 v*x*

   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 v*x***

   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).

Installing IA770 service pack 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.

To obtain the post-upgrade service pack file and documentation

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.
7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 software.

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 S8500 or S8700-series.

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 S8500 or S8700 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 S8500 or S8700 primary controller on page 499 if the primary controller is an S8500 or S8700-series.

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
- Administering the LSP Form

CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Telnet to the S8300, log in, and open a SAT session (type **sat** or **dsat**).
2. At the SAT prompt, type **`reset system 4`**

   The system reboots.
3. 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
 DiffServ/TOS PARAMETERS           Use Default Server Parameters? y
 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 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 Ehternet Port?
       Nework Region: 1
```

2. The field **Enable Ethernet Port?** should indicate `y` (yes)**.** The **Node Name** should be the IP address of the S8300 media server.

Administering the LSP Form

If the primary controller 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** screen, their status can be viewed with the **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **LSP** screen.

To add LSP names to the LSP screen

1. At the S8300 SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?        Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                      out-of-service
3      _____________                      out-of-service
4      _____________                      out-of-service
5      _____________                      out-of-service
6      _____________                      out-of-service
7      _____________                      out-of-service
8      _____________                      out-of-service
9      _____________                      out-of-service
10     _____________                      out-of-service
11     _____________                      out-of-service
12     _____________                      out-of-service
13     _____________                      out-of-service
14     _____________                      out-of-service
15     _____________                      out-of-service
16     _____________                      out-of-service
```

2. Enter the node name for each LSP supported by the primary controller and submit the form.

Skip to Administering the Media Gateway on page 506.

Administering an S8500 or S8700 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 S8500 or S8700 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 494 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
- Administering the LSP Form

Note:

For information on installing the CLAN boards on the S8500 or S8700 port networks and complete information on installing an S8700 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 S8700. For information on how to upgrade the firmware on the S8700, please see the section "Upgrade Firmware in Selected Port Cabinet Packs" in *Upgrading the Avaya media server Configuration* in the S8700 documentation portion of this documentation CD, "*Avaya S8300, S8500, and S8700 media server Library CD*," 555-233-325."

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 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 with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700 port networks, though they may also have the same network region.

The G700, in this case, 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 S8500 or S8700. The G700 network region may also differ because of the nature of the endpoints connected to it.

To define IP network regions for the G700 and CLAN board(s)

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. 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 S8500 or S8700 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:                  Home Domain:
    Name:
                                    Intra-region IP-IP Direct Audio: yes
AUDIO 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
 DiffServ/TOS PARAMETERS           Use Default Server Parameters? y
 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. 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 S8500 or S8700 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                                Page   3 of 19
                 Inter Network Region Connection Management

src dst   codec  direct                                  Dynamic CAC
rgn rgn    set    WAN   WAN-BW-limints  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 S8500 or S8700 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
LSP NAMES IN PRIORITY ORDER
1   node-10-LSP______
2   _________________
3   _________________
4   _________________
5   _________________
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 S8500 or S8700 port network CLAN boards

Note:

This should have already been established as a part of normal S8500 or S8700 installation.

1. Type **`change ip-interfaces`** to open the **IP Interfaces** screen.

IP Interfaces Screen

```
change ip-interfaces procr                                    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 Ehternet Port? y
       Nework Region: 1
               VLAN: 0

Number of CLAN Sockets Before Warning: 400
```

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 "*Administration for Network Connectivity for Avaya Communication Manager, 555-233-504"*.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
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.
Number of CLAN Sockets Before Warning	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.

3. Close the screen.

Administering the LSP Form

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 **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

To add LSP names to the LSP screen

1. At the SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?        Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                       out-of-service
3      _____________                       out-of-service
4      _____________                       out-of-service
5      _____________                       out-of-service
6      _____________                       out-of-service
7      _____________                       out-of-service
8      _____________                       out-of-service
9      _____________                       out-of-service
10     _____________                       out-of-service
11     _____________                       out-of-service
12     _____________                       out-of-service
13     _____________                       out-of-service
14     _____________                       out-of-service
15     _____________                       out-of-service
16     _____________                       out-of-service
```

2. Enter the node name for each LSP supported by the primary controller.
3. Submit the form.

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 and 250 for an S8500 or S8700).

   The S8300 displays the **Media Gateway** screen.

Add media gateway Screen

```
add media-gateway 1                                      Page  1 of 1
                           MEDIA GATEWAY
        Number: 1                              IP Address: 135.9.41.150
          Type: g700                FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                      MAC Address:
     Serial No: 012X06230551                 Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? n                  Controller IP Address:
                                                Site Data:
     Slot    Module Type                Name
      V1:
      V2:
      V3:
      V4:


      V8:
      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 S8500 or S8700 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                            IP Address: 135.9.41.150
          Type: g700               FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                    MAC Address: 00:04:0d:02:06:ca
     Serial No: 012X06230551                Encrypt Link? y
Network Region: 1                              Location: 1
    Registered? y                  Controller IP Address: 135.9.41.146
                                                Site Data:
     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/         IP Address/         Type   NetRgn
Reg?
                        FW Ver/HW Vint     Cntrl IP Addr

1        LabA           01DR07128730      135.177.49.57        g700    1       y
                        21 .13 .0  /0     135.177.49.59
2        Data MG2       02DR01130356      135.177.49.90        g350    1       n
                        11 .2  .0  /0     135.177.49.40
```

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 S8500 or S8700 system, this is a CLAN address; 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 S8700 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 looses 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 looses 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 S8500 or S8700 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 S8500 or S8700 alarms to notify the customer and services personnel that the network connection between the S8500 or S8700 and G700 has problems. If control passes to the LSP, the LSP’s license allows it to support the G700 endpoints for up to 10 days, within which the network problems should be resolved.

The customer must pass control back to the S8500 or S8700 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, in this case the S8500 or S8700.

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, S8500, or S8700/S8710 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 MultiService Network Manager
  - Avaya MultiService Network Manager
  - 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 445).

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, S8500, or S8700). 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.

Backing up the system

To back up the system

1. Make sure you have the IP address of the customer's FTP 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**, 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 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 site may have a different convention.

- **Host name**

  Enter the DNS name or IP address of the FTP 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 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 *Avaya IA770 INTUITY AUDIX Messaging, Release 3.0, Installation, Upgrades, and Troubleshooting*, 11-300532.

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 10: 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 Manger. 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
- Configure the G700
- Prepare to install firmware on the G700
- Install New Firmware on the G700 Media Gateway
- Administer Communication Manager
- Complete the Installation Process

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.

How is normal access to the S8300 and G700 provided

You can access the S8300 and G700 in several ways with either a direct connection or LAN connection.

Note:

Before the Upgrade Tool can be used to upgrade software on an LSP or firmware on a G700, as summarized below, the LSP must be administered on the primary controller.

Connecting directly to a target S8300

If you are at the location of the target S8300 (primary or LSP), you can connect directly to the S8300 Services port.

To install or upgrade directly

1. Install the S8300 software by:
   - Opening the Web interface and using the Avaya Installation Wizard

     or,
   - Opening the Web interface and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or the Upgrade Tool

     or,
   - Opening a telnet session to the S8300, and then telnet to the P330 stack processor

Connecting directly to the remote primary server (S8300, S8500, or S8700)

In this case, the target S8300 is an LSP. If you are at the location of the remote primary server, you can connect directly to the remote server's Services port.

To install or upgrade the target LSP remotely

1. Install the S8300 (LSP) software by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool
2. Upgrade the G700 firmware by:
   - Opening the Web interface and using the Avaya Installation Wizard or Upgrade Tool

     or,
   - Opening a telnet session to the primary server and then telnet to the P330 stack processor and perform the installation commands

Note:

For direct connections, the TFTP server must be on the Customer LAN, not on your laptop.

Connecting using the customer's LAN

If you can connect to the customer's LAN, you can:

1. Install the S8300 software by:
   - Opening the Web interface on the S8300 and using the Avaya Installation Wizard

     or,
   - Opening the Web interface on the S8300 and using the main menu
2. Upgrade the G700 firmware by:
   - Opening the Web interface on the primary server and using the Avaya Installation Wizard or Upgrade Tool

     or,
   - Opening a telnet session to the P330 stack processor and perform the installation commands

Note:

For LAN connections, the TFTP server can be your laptop or a customer computer on the LAN.

See About connection and login methods on page 47 for details on how physically to connect and log into the G700.

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:

- Collecting Installation Information
  - Getting the Serial Number of the G700, if Necessary
- Setting Up the TFTP Server on Your Laptop or on a Customer PC, if Necessary

Collecting Installation Information

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
- Type of system
- Equipment needed

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.

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, 1.3 to 2.0), you will need the serial number of the G700. To get this number, ask the customer's administrator to log in to the S8300 web page and select **View License Status** from the main menu to display the serial number.

For a new installation, 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.

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 31: Firmware file formats:

Note:

The latest firmware versions may different from those listed in Table 31. 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.

Table 31: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_0_17.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.0.4.exe
G700 Media Gateway	mgp<version id>	mgp_21_16_0.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v43.fdl
8-port DCP Media Module	mm712<version id>	mm712v5.fdl
24-Port DCP Media Module	mm717<version id>	mm717v2.fdl
8-port/trunk Analog Media Module	mm711<version id>	mm711h20v60.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v60.fdl
T1/E1 Media Module	mm710<version id>	mm710v9.fdl
8-port BRI Media Module	mm720<version id>	mm720v4.fdl
2-port BRI Media Module	mm722<version id>	mm722v2.fdl

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 **`nvram init`** to recondition the 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.

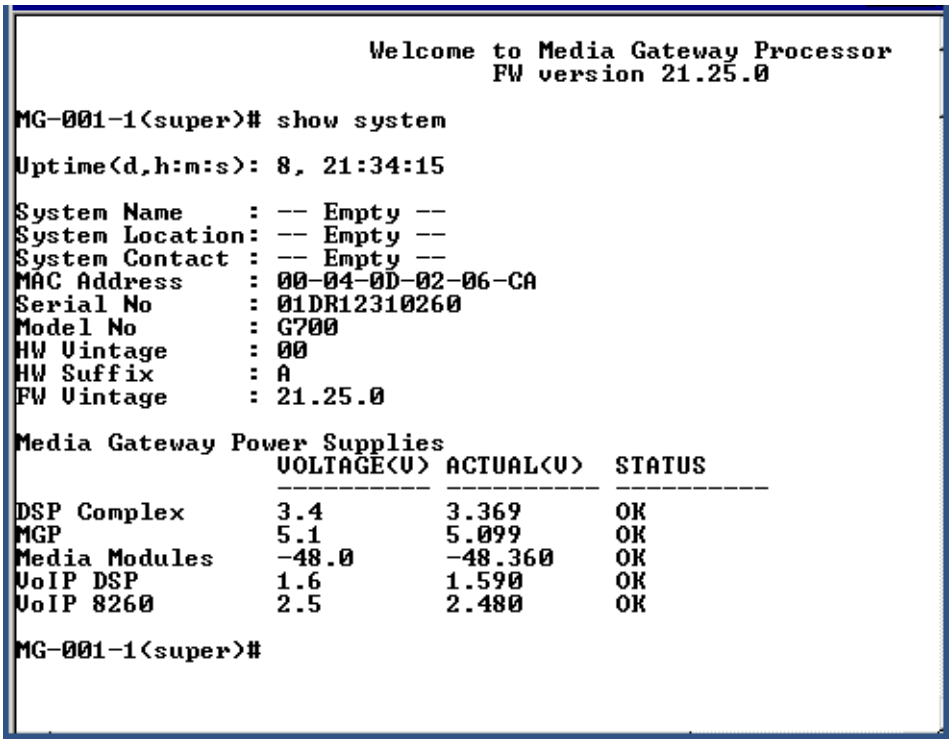
After you have configured the P330 stack processor, you assign an IP address to the G700 Media Gateway Processor (MGP). Your first task is to check the serial number of the MGP.

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



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 recondition the 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. Log in again at the **Welcome to P330** menu.
10. At the **P330-1(configure)#** prompt, type **session mgp**.
11. At the **MG-???-1(super)#** prompt, type **configure** to reach the configuration level of the command line interface.
12. 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

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>`*** is the IP address of the primary controller for this G700. If the primary controller is an S8700, this is the IP address of a C-LAN board that is connected to a pair of duplicated S8700/S8710s. If the primary controller is an S8300, this is 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 an S8700/S8710 duplicated pair or an S8300 configured as an LSP, depending on the G700's primary controller.

CAUTION:

If you need to change the mgc list, you must run **`clear mgc list`** before running **`set mgc list`** again.

Table 32 describes the possible optional controllers for an S8300 and S8700/S8710 primary controller:

Table 32: 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.
S8500 or S8700 or S8710	**First:** IP address of the C-LAN for the S8500 or S8700/S8710 primary controller. **Next three:** one, two, or three IP addresses of alternate C-LANs and/or LSPs.

Note:

For an S8500 or S8700/S8710 primary controller, the last three IP addresses in the list can be either the addresses of C-LANS (which are connected to the same S8500 or pair of S8700/S8710s that act as primary controllers) or addresses of LSPs. If you enter a combination of both, you must list C-LANs first and the LSPs last, *after* the C-LANs.

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 47 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 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   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.

Install New Firmware on the G700 Media Gateway

The procedures in this section install firmware on the G700 processors and media modules.

This section covers:

Installing New Firmware on the P330 Stack Processor

Installing new firmware on the G700 Media Gateway Processor

Installing new firmware on the media modules

Following these procedures, Setting rapid spanning tree on the network enables a loop avoidance protocol on the network.

Manually installing G700 and media modules firmware

Installing New Firmware on the P330 Stack Processor

To install P330 stack processor firmware

1. 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

```
FLASH MEMORY     IMAGE VERSION
Bank A           109
Bank B           210

ACTIVE NOW       ACTIVE AFTER REBOOT
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 S8500 or S8700-series Media Server.

Perform one of the following two administration procedures in this section:

- Administering an S8300 primary controller
- Administering an S8500 or S8700/S8710 primary controller

Administering an S8300 primary controller

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
- Administering the LSP Form

CAUTION:

Before continuing, be sure you have saved translations in Communication Manager.

Begin by resetting the system.

To reset the System

1. Telnet to the S8300, log in, and open a SAT session (type **sat** or **dsat**).
2. At the SAT prompt, type **`reset system 4`**

   The system reboots.
3. 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
 DiffServ/TOS PARAMETERS           Use Default Server Parameters? y
 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 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 Ehternet Port?
       Nework Region: 1
```

2. The field **Enable Ethernet Port?** should indicate y (yes)**.** The **Node Name** should be the IP address of the S8300 media server.

Administering the LSP Form

If the primary controller 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** screen, their status can be viewed with the **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the **LSP** screen.

To add LSP names to the LSP screen

1. At the S8300 SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?        Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                      out-of-service
3      _____________                      out-of-service
4      _____________                      out-of-service
5      _____________                      out-of-service
6      _____________                      out-of-service
7      _____________                      out-of-service
8      _____________                      out-of-service
9      _____________                      out-of-service
10     _____________                      out-of-service
11     _____________                      out-of-service
12     _____________                      out-of-service
13     _____________                      out-of-service
14     _____________                      out-of-service
15     _____________                      out-of-service
16     _____________                      out-of-service
```

2. Enter the node name for each LSP supported by the primary controller and submit the form.

Skip to Administering the Media Gateway on page 557 to continue.

Administering an S8500 or S8700/S8710 primary controller

Complete the procedures in this section if the primary controller for the G700 you are installing is an S8500, S8700 or S8710. If the primary controller is an S8300, you should have completed the procedures in Administering an S8300 primary controller on page 545.

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
- Administering the LSP Form

Note:

For information on installing the CLAN boards on the S8500 or S8700 port networks and complete information on installing an S8700 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 S8700. For information on how to upgrade the firmware on the S8700, please see the section "Upgrade Firmware in Selected Port Cabinet Packs" in *Upgrading the Avaya media server Configuration* in the S8700 documentation portion of this documentation CD, *Documentation for Avaya Communication Manager, Media Gateways and Servers CD*, 03-300151.

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 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 with thousands of telephones in the network. In this case, you define a network region for each CLAN board on the S8500 or S8700 port networks, though they may also have the same network region.

The G700, in this case, 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 S8500 or S8700. The G700 network region may also differ because of the nature of the endpoints connected to it.

To define IP network regions for the G700 and CLAN board(s)

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. 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 S8500 or S8700 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:                  Home Domain:
    Name:
                                    Intra-region IP-IP Direct Audio: yes
AUDIO 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
 DiffServ/TOS PARAMETERS           Use Default Server Parameters? y
 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. 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 S8500 or S8700 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                                Page   3 of 19
                 Inter Network Region Connection Management

src dst   codec  direct                                  Dynamic CAC
rgn rgn    set    WAN   WAN-BW-limints  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 S8500 or S8700 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
LSP NAMES IN PRIORITY ORDER
1   node-10-LSP______
2   _________________
3   _________________
4   _________________
5   _________________
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 S8500 or S8700 port network CLAN boards

Note:

This should have already been established as a part of normal S8500 or S8700 installation.

1. Type **`change ip-interfaces`** to open the **IP Interfaces** screen.

IP Interfaces Screen

```
change ip-interfaces procr                                    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 Ehternet Port? y
       Nework Region: 1
               VLAN: 0

Number of CLAN Sockets Before Warning: 400
```

2. Complete the fields as described the in Table 33.

Table 33: 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 "*Administration for Network Connectivity for Avaya Communication Manager, 555-233-504"*.
Gateway Address	The address of a network node that serves as the default gateway for the IP interface.
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.
Number of CLAN Sockets Before Warning	The threshold for the number of sockets used by this C-LAN that triggers a warning message to be sent to the error log.

3. Close the screen.

Administering the LSP Form

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 **`display lsp`** command.

Note:

The LSP node names must be administered on the node-names-ip form before they can be entered on the LSP form.

To add LSP names to the LSP screen

1. At the SAT prompt, type **`change lsp`** to open the **LSP** screen.

LSP Screen

```
change lsp                                              Page   1 of   16
                          LOCAL SURVIVABLE PROCESSOR
Number NAME           IP Address             Service      Translations
                                              State?         Updated
1      node-10-LSP    192.168.1.50            in-service   14:21 5/4/2003
2      _____________                       out-of-service
3      _____________                       out-of-service
4      _____________                       out-of-service
5      _____________                       out-of-service
6      _____________                       out-of-service
7      _____________                       out-of-service
8      _____________                       out-of-service
9      _____________                       out-of-service
10     _____________                       out-of-service
11     _____________                       out-of-service
12     _____________                       out-of-service
13     _____________                       out-of-service
14     _____________                       out-of-service
15     _____________                       out-of-service
16     _____________                       out-of-service
```

2. Enter the node name for each LSP supported by the primary controller.
3. Submit the form.

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 and 250 for an S8500 or S8700).

   The S8300 displays the **Media Gateway** screen.

Add media gateway Screen

```
add media-gateway 1                                      Page  1 of 1
                           MEDIA GATEWAY
        Number: 1                              IP Address: 135.9.41.150
          Type: g700                FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                      MAC Address:
     Serial No: 012X06230551                 Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? n                  Controller IP Address:
                                                Site Data:
     Slot    Module Type                Name
      V1:
      V2:
      V3:
      V4:


      V8:
      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 S8500 or S8700 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                            IP Address: 135.9.41.150
          Type: g700               FW Version/HW Vintage: 21.13.0 /0
          Name: Swainsons                     MAC Address: 00:04:0d:02:06:ca
     Serial No: 012X06230551                 Encrypt Link? y
Network Region: 1                               Location: 1
    Registered? y                  Controller IP Address: 135.9.41.146
                                                Site Data:
     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/        IP Address/        Type   NetRgn
Reg?
                      FW Ver/HW Vint    Cntrl IP Addr

1        LabA         01DR07128730     135.177.49.57       g700    1       y
                      21 .13 .0  /0    135.177.49.59
2        Data MG2     02DR01130356     135.177.49.90       g350    1       n
                      11 .2  .0  /0    135.177.49.40
```

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 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware

About upgrading an existing S8300A to R3.0

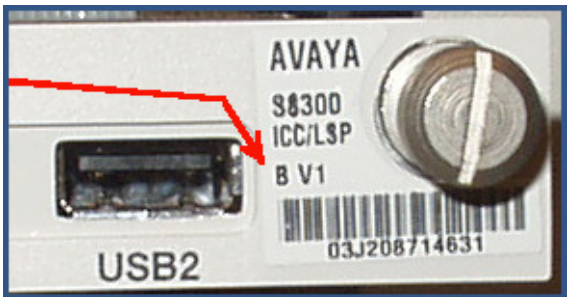
This chapter covers the procedures to upgrade the Communication Manager software to release 3.0 on an installed Avaya S8300 Media Server, version A. The procedures to upgrade the G700 firmware use CLI commands instead of the Upgrade Tool. The current Communication Manager release can be any pre-2.1 release. These procedures require replacing version A of the S8300 with version B. 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. If the currently installed S8300 is version B, follow the upgrade procedures in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware.

The B version of the S8300 shows a “B” on the faceplate (see Figure 44: S8300B version faceplate) — the version is not indicated on the faceplate of the A version.

Figure 44: S8300B version faceplate



The S8300 version can also be determined with the SAT command, `list config all`. The B version is listed as **S8300B**. 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 S8500 or S8700/S8710 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. 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.

Release 3.0 upgrade scenarios

The upgrade procedures are slightly different depending on the upgrade scenario. The main differences between the scenarios are summarized in Table 34 and are noted in the detailed procedures.

Table 34: Release 3.0 upgrade scenarios

Upgrade From	S8300 B Hard Drive has Remastering Software Only	S8300 B Hard Drive has R2.0.x Software Installed
R 1.x	Linux Migration backup Remaster and upgrade View/Restore Data	Linux Migration backup Upgrade View/Restore Data
R 2.x	Backup Now Remaster and upgrade View/Restore Data	Backup Now Upgrade View/Restore Data
	Move hard drive from A to B Upgrade	

The unshaded cells in this table are the most common and recommended upgrade scenarios. The shaded cells are scenarios that are unlikely or not recommended.

The new S8300B media server will normally not have Communication Manager software installed on it. If it does, remastering the hard drive is still recommended but could be replaced with a standard upgrade.

If the current system has a 2.0.x release of Communication Manager installed, it is possible to move the hard drive from the S8300A to the S8300B and then upgrade to 3.0. This saves a few steps but it is not recommended for the following reasons:

- If the S8300A hard drive is not moved, it provides a means to quickly revert to the original configuration, if necessary.
- Hardware could be damaged in the process of changing hard drives.
- Only the Fujitsu hard drives can be moved.
- The hard drives on the S8300B have a larger capacity than the hard drives on S8300A. This larger capacity is not needed for R 3.0 but may be needed in the future.

Accessing the Server CD

The R3.0 Communication Manager software and other files needed for the R3.0 upgrade are on the Server CD that you take to the customer site. You can make the Server CD available to the upgrade process in one of two ways:

- ***Recommended:*** Place the CD in the CD-ROM drive on the technician's laptop. This method requires that the Avaya TFTP Server software (available at support.avaya.com) is installed on the technician's laptop. In addition, this method requires that the S8300B ***does not*** have Communication Manager software installed on its hard drive.

  or,

- Place the CD in an external USB CD-ROM drive connected to one of the USB ports on the S8300 faceplate. This method works whether or not Communication Manager software is installed on the S8300B hard drive.

  Important:

  Before you go to the site, either you must have the TFTP server installed on your laptop (recommended), or you must have an external USB CD-ROM drive.

  The new S8300B will normally not have Communication Manager software installed on its hard drive. You should check the S8300B that you will be installing (or ask the customer to check) before going to the site to determine whether you need to have the external USB CD-ROM drive.

  - If software is not installed, the label on the hard drive will say "S8300B Hard Drive Without CM Software."
  - If software is installed, the label will indicate the software release.

    In this case, you must use the external USB CD-ROM drive because the TFTP server on your laptop will not work.

This chapter describes the upgrade procedure with the TFTP Server software installed on the laptop and using the laptop CD-ROM drive as source of the upgrade software. For instructions on obtaining and installing the Avaya TFTP Server, see Appendix D: Install the Avaya TFTP server.

Accessing the S8300

To access the S8300 on-site, you normally connect the technician's laptop directly to the Services port on the S8300 using a crossover cable. See About connection and login methods on page 47 for instructions on accessing the S8300 and G700.

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.

Do the following procedures:

- Installing TFTP server or obtaining USB CD-ROM drive on page 567

  Important:
  If the new S8300B that you will be installing has Communication Manager software installed on its hard drive, you must use an external USB CD-ROM drive instead of the TFTP server on your laptop. See Accessing the Server CD on page 565 for more information.

- Installing TFTP server or obtaining USB CD-ROM drive on page 567
- Planning forms provided by the project manager on page 567
- Getting the serial number of the G700, if necessary on page 568
- Checking the number of allocated ports on page 568
- Identifying the FTP server for backing up data on page 568
- Obtaining S8300 software and G700 firmware on page 569
- Obtaining service pack files, if needed on page 570
- If using IA770, checking stored messages size, obtaining service pack (or RFU) and language files on page 571
- Completing the RFA process (obtaining license and authentication files) on page 573

Installing TFTP server or obtaining USB CD-ROM drive

Upgrading Communication Manager on an S8300 to release 3.0 normally requires remastering the S8300B hard drive. After remastering the drive, the remastering program looks for the Communication Manager software files on:

- An external USB CD-ROM drive, or
- The laptop, if a TFTP server is installed

You must have either the Avaya TFTP server software installed on your laptop or take a USB CD-ROM drive to the site. If you do not already have the Avaya TFTP server installed on your laptop, you can obtain the software from the Avaya Support website and install it as described in Appendix D: Install the Avaya TFTP server.

Important:
If the new S8300B that you will be installing has Communication Manager software installed on its hard drive, you must use an external USB CD-ROM drive instead of the TFTP server on your laptop. See Accessing the Server CD on page 565 for more information.

Collecting upgrade information

Filling in the EPW, if upgrading from release 1.1

If you are upgrading from release 1.1, you will need to do a complete configuration of the S8300B after the upgrade to release 3.0. 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/avayaiw/ 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.

Planning forms provided by the project manager

The Project Manager should provide you with forms that contain all the information needed to prepare for this installation. The information includes IP addresses, subnet mask addresses, logins, passwords, people to contact, the type of system, and 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.

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 3.0 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.

Identifying the FTP server for backing up data

During the installation and upgrade procedures, you will need to back up the system data to an FTP server. Normally, you will use an FTP server on the customer's LAN for backups.

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

Check with your project manager or the customer for this information.

Important:
Before going to the customer site, make sure that you can use a customer server for backups.

Obtaining S8300 software and G700 firmware

The file containing the software for the S8300 has a *.tar extension and contains both the S8300 software and the G700 and media module firmware. The *.tar file is on a CD-ROM that you take to the site. This CD is called the “Server CD” because it contains software for all of the Linux servers. Additional files that may be needed are license and authentication files, and the most recent versions of the software service pack files and G700 firmware files.

The process for upgrading to release 3.0 of Communication Manager varies slightly, depending on the release from which you are upgrading.

Table 35: R3.0 Upgrade requirements depending on pre-upgrade release

Software Release Before Upgrade to Release 2.1	Upgrade Requirement
Release 1.1.x and all other 1.x.x releases not listed below R011x.01.xxx.x	No pre-upgrade service pack required. You need to back up only translation files. Once the hard drive is remastered and the new software is installed on the S8300B, you must reconfigure the media server as if it were a new installation using the Avaya Installation Wizard.
Release 1.2.x, 1.3.0. 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, you can restore all the files using LMBR*.
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, 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. Back up the system and translations files using Data Backup/Restore†. Once the hard drive is remastered and the new software is installed on the S8300B, you can restore the files using Data Backup/Restore.

*. The LMBR backup contains backup sets for the translations, OS and system files.

†. The Data backup contains backup sets for the translations, OS and system files, security files, and AUDIX data, if any

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.

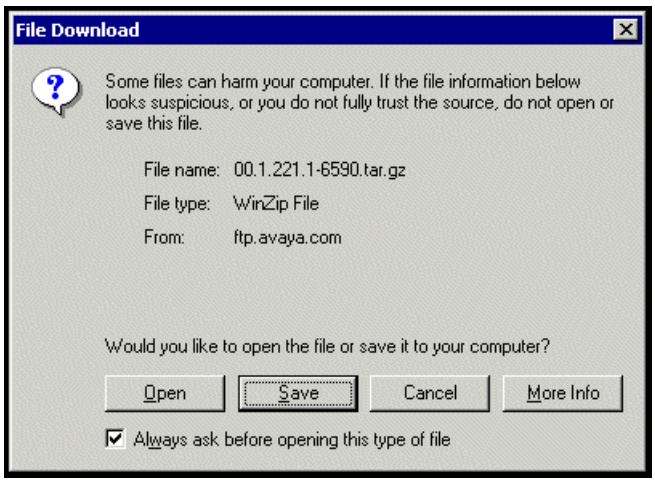
To download a service pack

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 3.0**).
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.

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 03.0.526.5-1003.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.

If using IA770, checking stored messages size, obtaining service pack (or RFU) and language files

If IA700 is installed, check the size of stored messages, determine whether an service pack is needed, and/or optional languages are used.

When upgrading Communication Manager to release 3.0 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.

Checking the size of stored messages

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 and documentation can be found on the Avaya Support Web Site at http://support.avaya.com.

To obtain the post-upgrade service pack file and documentation

1. On the Avaya Support website, double click on **Messaging** in the list on the left.
2. Scroll down to the INTUITY links and double click on **IA 770 INTUITY AUDIX Messaging Application**.
3. Double click on **All Documents**.
4. 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**.
5. Double click on the file name.

   For example, **C6039rf+c.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.
7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 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 obtain the appropriate language CD(s) and take them to the site.

Completing the RFA process (obtaining license and authentication 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 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, S8500, S8700, S8710, or Blade 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.

Preparing for the upgrade to R3.0 on-site

When you arrive on-site, you must perform the following tasks in preparation for the upgrade to release 2.1:

- Accessing the S8300 on page 576
- Checking current software release on page 577
- Pre-Upgrade Tasks — If the S8300 is the primary controller on page 578
- Getting IA770 data and stopping IA770 (if IA770 is being used) on page 582
- Backing up system files on page 585
- Recording configuration information on page 588

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. You will use both Telnet and the Maintenance Web Interface to perform the procedures.

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 48.

To access the S8300 using telnet

1. Click **Start > Run** to open the Run dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.
3. Log in as **craft** or **dadmin**.

   Accept the defaults for Suppress Alarm Origination (`y`) and Terminal Type (`vt100`). At this point, you get the bash prompt and can enter CLI commands.

To access the S8300 using the Maintenance Web Interface

1. Launch the Web browser.
2. 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**.

To access the SAT

1. From the bash CLI, type **SAT** and press **Enter**.

   Or, to open SAT directly from your laptop,

   a. Click **Start > Run**.

   b. Type **telnet 192.11.13.6 5023** and press **Enter**.
2. Log in as *craft* or *dadmin*.
3. Enter **w2ktt** for the **Terminal Type** (if you are running Windows 2000 on your laptop).
4. Accept the default (y) for **Suppress Alarm Origination**.

Checking current software release

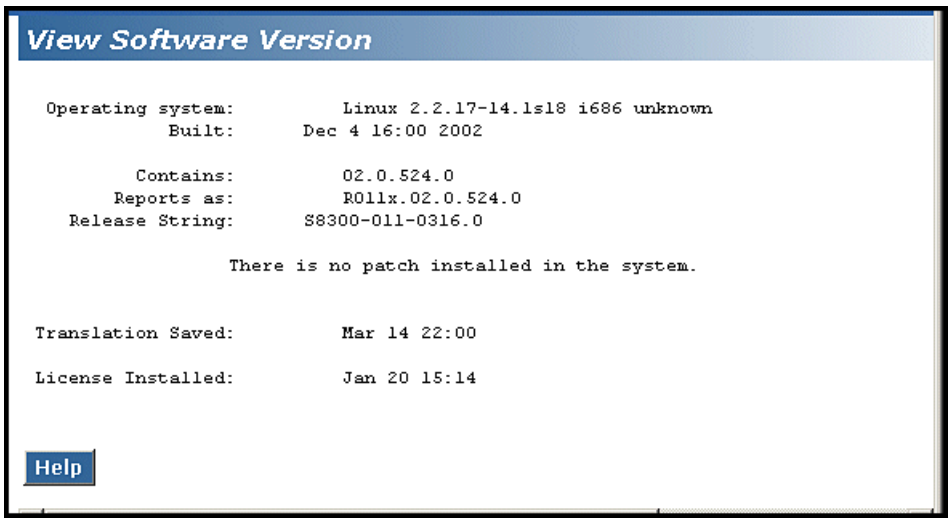
Check the release of Communication Manager currently running on the S8300 to determine whether a pre-upgrade service pack is required.

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 36 maps the release number to the **Reports as:** field, and specifies whether or not a pre-upgrade update is required.

Table 36: 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
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

Pre-Upgrade Tasks — If the S8300 is the primary controller

Skip to Upgrading the S8300A on page 589, 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 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 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 585 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

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.

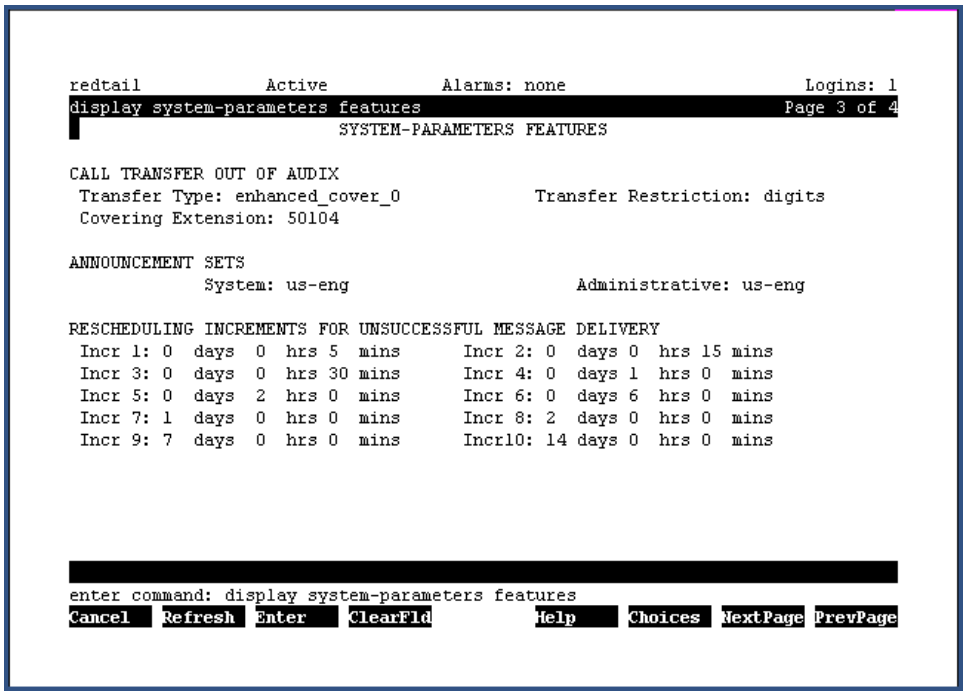
Determining whether optional languages are needed

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



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.

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.

A770 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 3.0 system. If any other language files are listed, you will need to download the additional language files from a language CD after the upgrade.

Stopping IA770

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.

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 1.1.x or 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

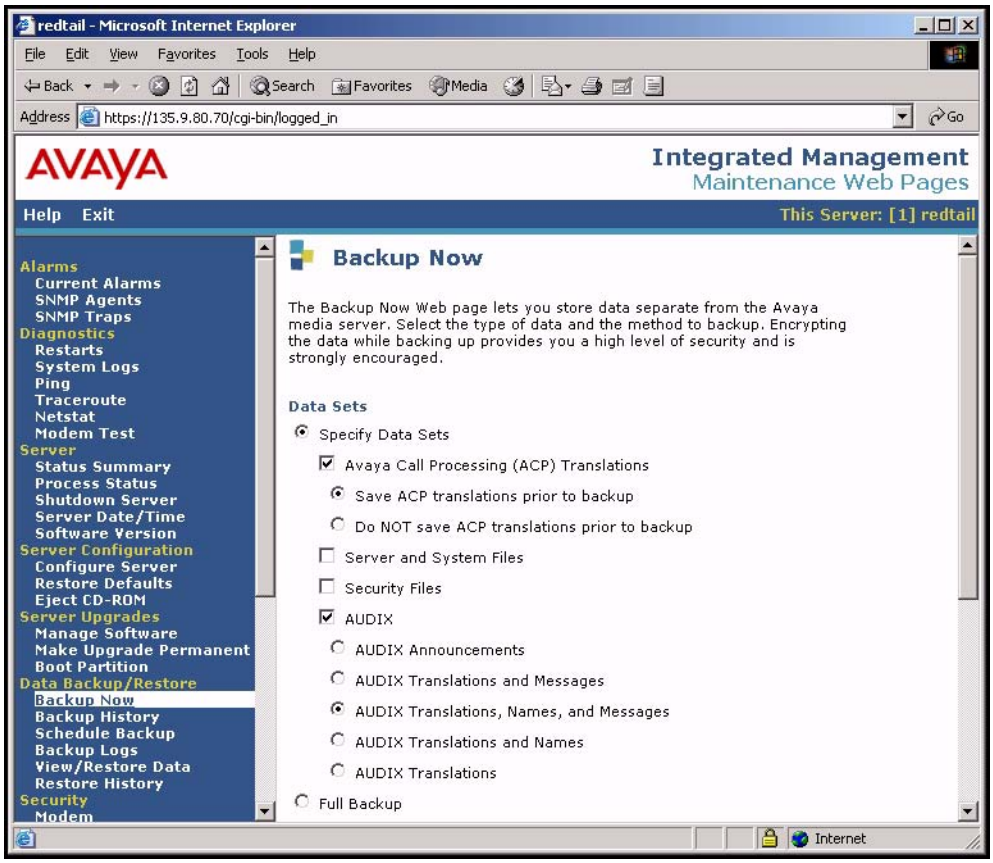
1. On the Maintenance Web Interface under Data Backup/Restore, click **Backup Now**.

   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 this option only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

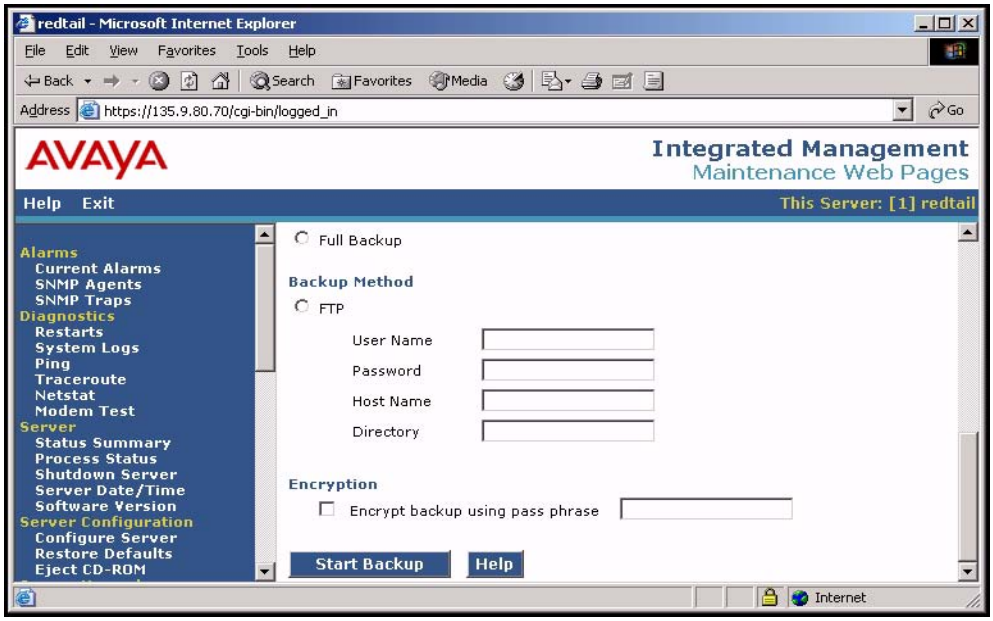
   - Server and System Files
   - Security Files

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.

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 1.2 or later, most of the configuration data will be re-entered automatically with the restore process. However, if you are upgrading from a pre-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.

7. If upgrading from 1.2 or later, record the data displayed on the **Configure Interface** screen:
   - Server IP address
   - Gateway IP address,
   - Subnet mask

   You can skip the remaining configuration screens.
8. If upgrading from pre-1.2 release, record the data from all configuration screens.

Upgrading 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 3.0.

Upgrading an S8300 to release 3.0 requires removing the S8300A and replacing it with an S8300B. The new S8300B should have the remastering program (RP) software installed on its hard drive. The remastering program remasters the hard drive and installs the R 3.0 Communications Manager software. These procedures are described in this section.

This section covers:

- Installing the pre-upgrade software service pack, if necessary on page 589
- Linux migration backup (if current release is 1.2.0 through 1.3.x) on page 592
- Replacing the S8300A with the S8300B Media Server on page 595
- Upgrading the S8300B Media Server on page 596

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 **1.1.0** and **1.1.9**, or between **2.0.0** and **2.0.9**, skip this service pack installation procedure and go to Replacing the S8300A with the S8300B Media Server on page 595.

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 592.

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 590.

Current release is 2.x, use To install the pre-upgrade service pack when the current release is 2.x. on page 591

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, **03.0.526.5-1003.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, **03.0.526.5-1003**. 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 Manger** 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 Media Server on page 595 if the current software release is 2.x. If you are upgrading from a 2.x release, the Linux Migration Backup may not work. After the upgrade, you will restore data from the system backup you did earlier.

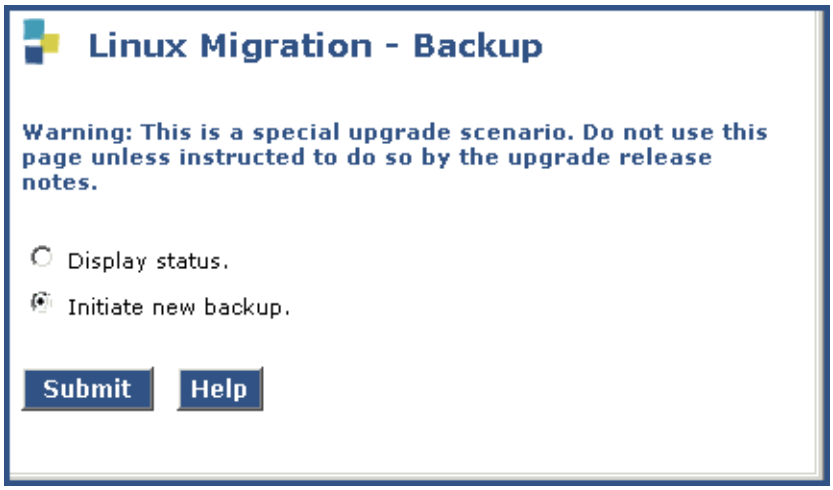
In this section, you will use the Linux Migration Backup procedure on the Maintenance Web Interface to save the system files and translations. After the upgrade, you will use the Linux Migration Restore feature to restore these files.

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.

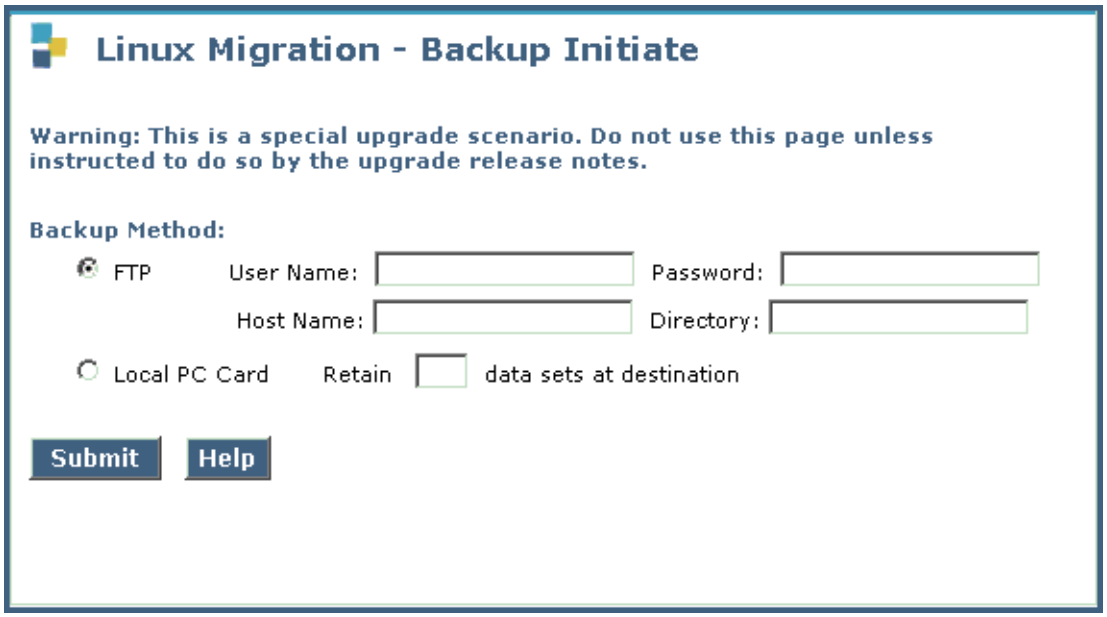
Linux Migration - Backup screen



2. Select "Initiate new backup or restore" and click **Submit**.

   The **Linux Migration - Backup Initiate** screen displays.

Linux Migration - Backup Initiate screen



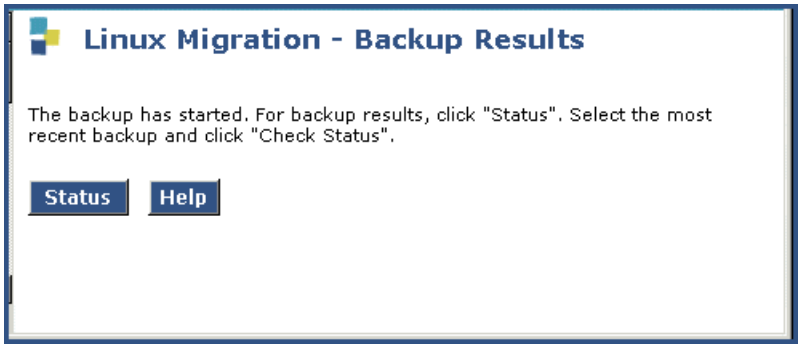
3. Under Backup Method, select FTP

   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

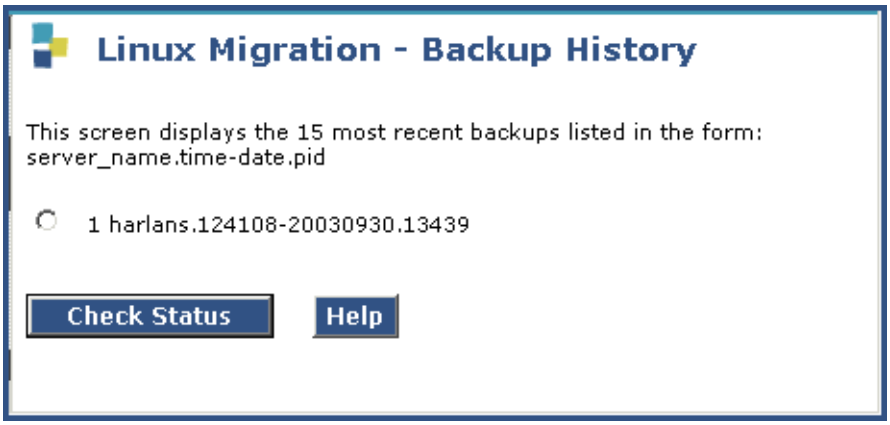


4. Click **Status** to see the backup progress.

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**.

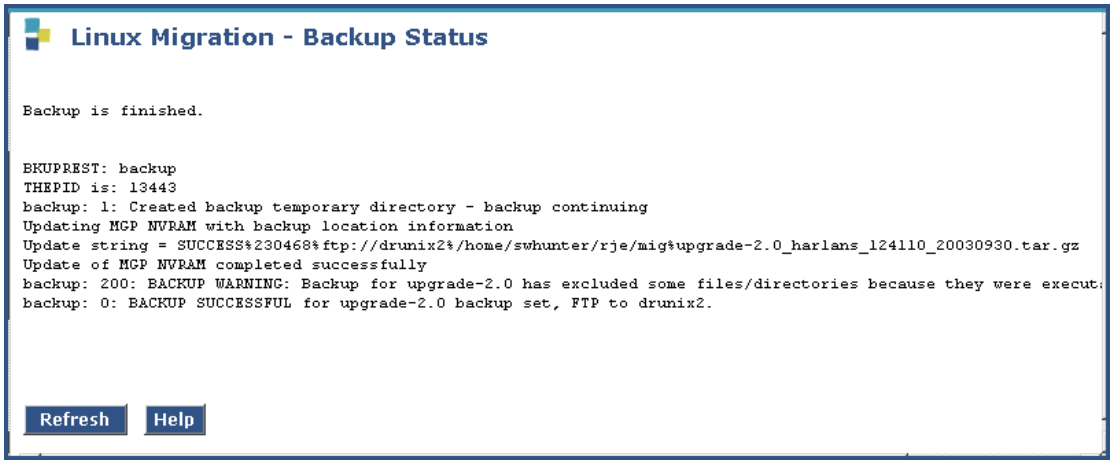
Linux Migration - Backup History screen



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 Media Server

To remove the S8300A and insert the S8300B

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 S8300 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 S8300A, move it from the S8300A to the S8300B.

   Note:

   The CWY1 unit and its associated integration is supported for upgrades of existing installations.
8. The LED panel (above slot V1) must be reinserted together with the S8300 circuit pack.
   a. 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.
   b. 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.
9. 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.
10. Reconnect the laptop to the services port of the new S8300B.

Upgrading the S8300B Media Server

- Setting telnet parameters on page 596
- Remastering the hard drive and installing the upgrade software on page 597
- Verifying software version on page 602
- Copying files to the S8300 on page 603
- Configuring network parameters on page 605
- Verifying connectivity on page 606
- Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) on page 608
- Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x) on page 609
- Verifying the time, date, and time zone on page 613
- Verifying media server configuration on page 613
- Installing the new license file on page 615
- Installing the new authentication file, if any on page 616
- Saving translations (if not using IA770 and S8300 is not an LSP) on page 617
- Verifying operation on page 617

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 hard drive and installing the upgrade software

To do before you start the upgrade

1. Verify that the S8300B 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.
5. Insert the Unity CD in the CD-ROM drive:

   - If TFTP server software is installed on your laptop, ***start the TFTP server program*** (TFTPServer32.exe), and insert the Communication Manager unity CD in the laptop's CD drive.

     CAUTION:

     Verify good AC power connections to the laptop. Do not attempt a remastering using only the laptop's battery power.

   Note:

   Shut down all applications on the laptop except for the TFTP server and the telnet client. Other background applications can overly use laptop resources.

   Note:

   Ensure that the **Outbound file** path is set to the root of your laptop's CD-ROM drive. (For example, D:\)

   To check:

   i. Open the **System** menu in the TFTP server program

   ii. Select **Setup**

   iii. Open the **Outbound** tab.

   iv. To change the **Outbound file** path, click the **Browser** button and select the **CD** drive.

   or,

   - If your laptop does not have TFTP server software installed, attach an external USB CD-ROM drive to one of the USB ports on the S8300B and insert the Unity CD in the drive.

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.

NOTE: If you get the login prompt instead of the RP screen

If the telnet login prompt appears instead of the RP screen, the hard drive contains a Communication Manager software release. In this case, if you have a USB CD-ROM drive, connect the drive to a USB port on the S8300 and insert the unity CD. Then log in to the telnet session (using the initial *craft* login) and use the **Shutdown Server** feature on the Maintenance Web Interface to reboot the system. After the reboot completes, telnet to 192.11.13.6 and the RP screen should now be displayed.

If you do not have the USB CD-ROM, you cannot proceed with the upgrade procedure described in this chapter. However, you can upgrade the Communication Manger software using the procedure described in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware and then return to this chapter.

To upgrade using the procedure in Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware

1. Complete the procedures starting at Installing the pre-upgrade software service pack on page 658 and ending with Making the upgrade permanent on page 670. Note that you must have a copy of the license and authentication files on your laptop and install them before doing the upgrade.
2. Return to this chapter and complete the procedures starting with Verifying software version on page 251, using the initial *craft* login.
3. Complete all the remaining procedures ***except*** installation of the license and authentication files, which was done in step 1.

Alternatively, you can obtain a USB CD-ROM drive or an S8300B with only the RP software and proceed from Remastering the hard drive and installing the upgrade software on page 245.

The first RP screen

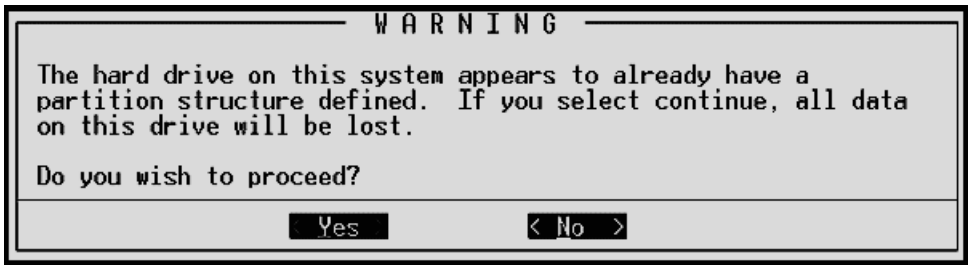
Tip:

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.

4. Select **Install** and press **Enter**.

   If a **Warning** screen appears,

RP Warning screen

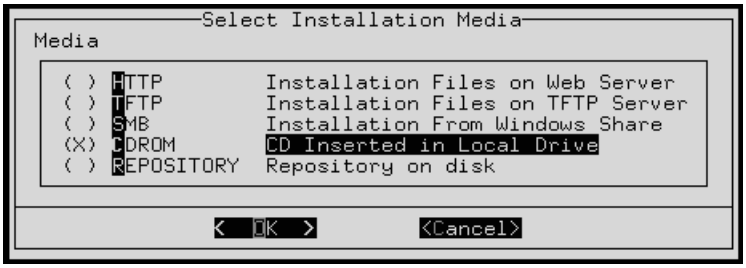


select **Yes** and press **Enter**.

Note:

At this point, the installation script looks for the Unity CD either on your laptop or in a CD drive connected to the USB port. If you do not have the TFTP server running on the laptop, and a CD drive is not attached to a USB port, you will see the **Select Installation Media** screen:

The Select Installation Media screen



If you see the Select Installation Media screen:

a. Start up the TFTP server on your laptop, or connect a USB CD-ROM drive to one of the USB ports.

b. Insert the unity CD in the laptop or USB drive.

c. Select either **TFTP** or **CDROM**.

d. Select **OK,** and press **Enter**.

The **Select Release Version** screen appears.

The Select Release Version screen

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

6. The **Run AUDIX Installation** screen appears.

Run AUDIX Installation screen

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

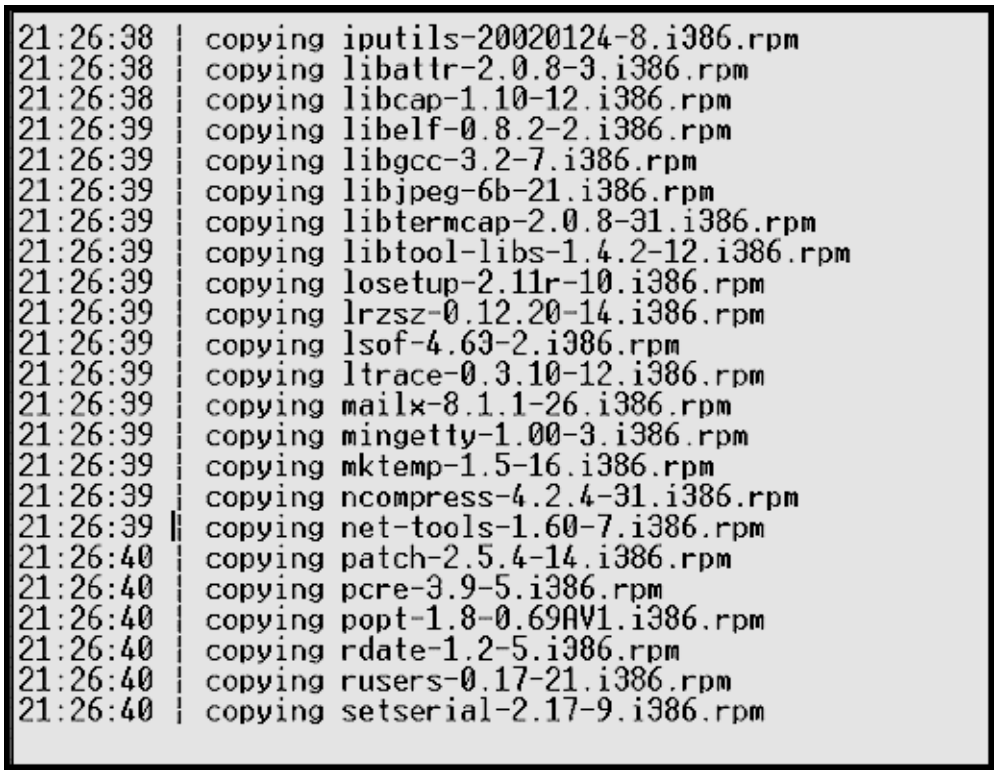
   At this point, the following processes are initiated:

   a. The S8300 hard drive is 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



These processes take 15–30 minutes. When the media server is ready to reboot, the following screen flashes for about 5 seconds.

Software and firmware update reminder

When the installation is complete, the CD drive door opens and the system reboots automatically. The reboot takes 1–3 minutes.

In the event you used the laptop TFTP server and you have a problem with power and the S8300 does not reboot, there are two methods of recovery:

- Use the USB CD-ROM to plug into the S8300 and repeat the remastering process using the Unity CD.
- Arrange access to another hard drive (comcode 700307028) should it be necessary to perform the TFTP remaster procedure on it.

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 on to Integrated Management and launch the Maintenance Web Interface.
2. Under Server, click **Software Version**.
3. Verify that the media server is running Release 3.0 software.

   The **Report as:** string should show **R013x.01** at the beginning of the string. For example, **R013x.01.0.340.3**.

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

During reformatting of the hard drive, a new directory, /var/home/ftp/**pub**, was created. For release 2.0 and later, this *pub* directory will be used as the /var/home/ftp directory that was used in previous releases.

You must copy the remaining required files to the pub directory on the S8300 hard drive. This includes, but is not limited to:

- the post-upgrade service pack file
- License file
- Avaya authentication file (if needed)
- New firmware files

Note:

If you are copying a license file or authentication file, be sure the /var/home/ftp/pub directory contains no files with a *.pwd or *.lic extension. There should be only one of each of these file types this directory. If any of these file types exist in the pub directory, move, rename, or delete them before you copy the new files.

To copy files to the S8300

1. Log on to Integrated Management and launch the Maintenance Web Interface.

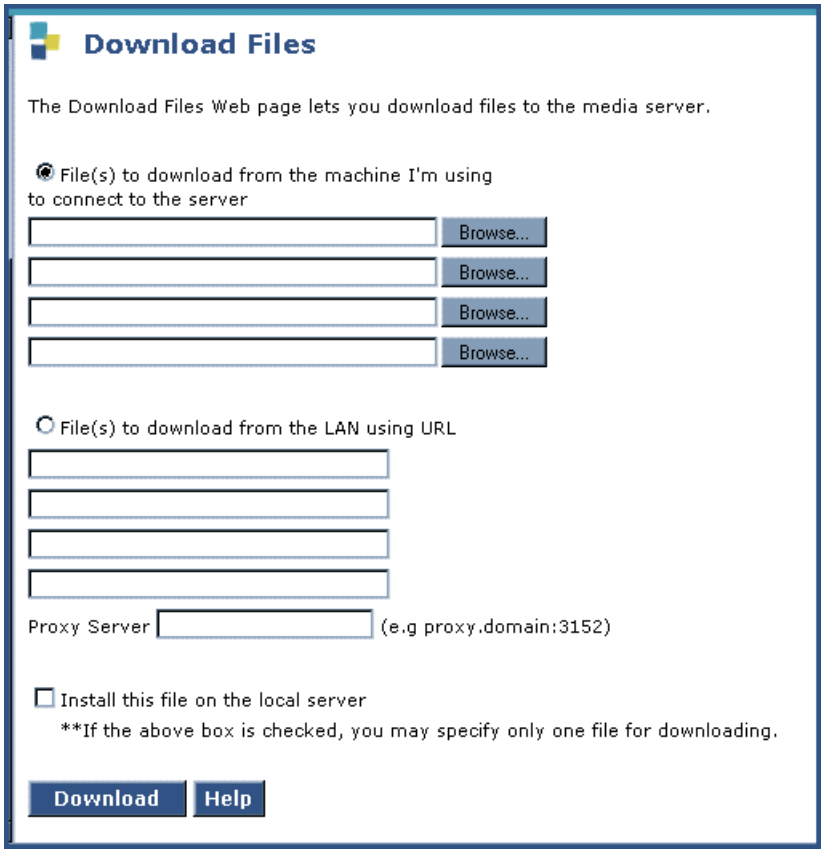
   Note:

   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.)

2. Under Miscellaneous click **Download Files**.

   The **Download Files** screen displays.

Download Files screen



3. 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 are downloading an IP Telephone software file, download this file last with the **Install this file on the local server** checkbox **checked**. Note that the software file must be in a special .tar format to use this feature. See *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507, for information about installing IP Telephone software.

   Note:

   To manually FTP files from your laptop to /var/home/ftp/pub, you must `cd` to pub after starting ftp and logging in; that is, type `cd pub`.

4. 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 Server CD from the CD drive.

Configuring network parameters

Note:

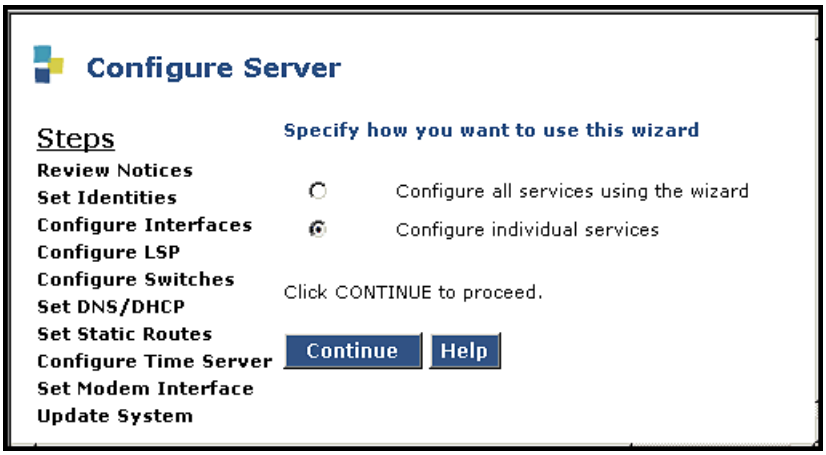
For this procedure, you must have the host name, subnet mask, and IP address of the S8300, and the IP address of the default gateway.

Because the software upgrade resets the configuration data, you must reconfigure the network parameters on the S8300 before restoring the backup files. Also, it is possible that the new software added or changed some of the configuration fields or screens.

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.

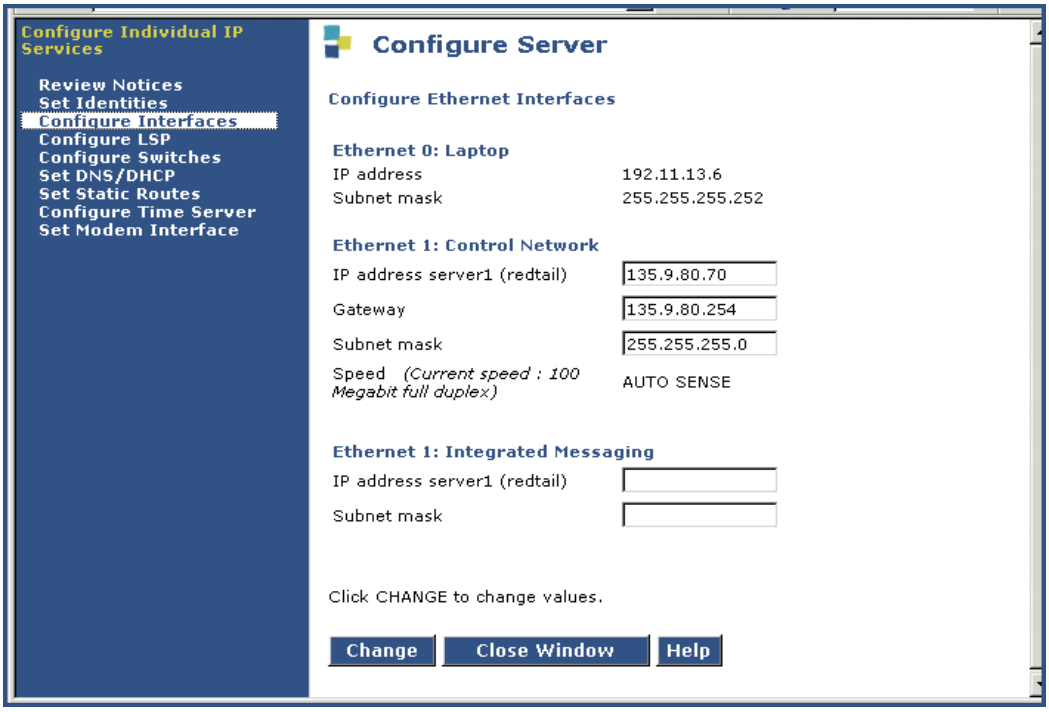
Specify how you want to use this wizard screen



3. Select **Configure individual services** and click **Continue**.
4. Click **Configure Interfaces** from the “Configure Individual IP Services” list on the left.

   The **Configure Ethernet Interfaces** screen displays.

Configure Ethernet Interfaces screen



5. Fill in the correct server IP address, Gateway, and Subnet mask.

   If these fields are already filled in, overwrite them with the correct information. Leave the Integrated Messaging fields 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.

6. 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 Linux-Migration backup file is 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.

Installing post-upgrade Communication Manager service pack file from your laptop

CAUTION:

The software service pack may or may not be call-preserving.

Note:

Skip this procedure if there is no Communication Manager service pack file to install.

This service pack may or may not be call preserving.

Use a telnet session to install the service pack file.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **`telnet 192.11.13.6`** and press **Enter**.
3. Log in as **craft**.
4. Type **`cd /var/home/ftp/pub`** and press **Enter** to access the pub directory.
5. At the prompt, type **`ls -ltr`** and press **Enter** to list files in the pub directory.

   The media server displays a list of files in the FTP directory. Verify that the directory contains the Communication Manager .tar.gz file you have uploaded, if any.
6. Type **`update_unpack`** ***`update.tar.gz`***, where ***`update`*** is the release or issue number of the latest software update file. (For example, **`00.0.339.4-xxxx.tar.gz`**). Press **Enter**.
7. Type **`update_show`** and press **Enter** to list Communication Manager files to verify the new software update file was unpacked.
8. Type **`update_activate`** ***`update`***, where ***`update`*** is the release or issue number of the latest software update 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 (reset system 4). 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 software update (patch) was applied.
9. Type **`update_show`** again and press **Enter** to list Communication Manager files to verify the new software update file was activated.

Restoring data

In this section you will restore the system data that you backed up. Do ***only one*** of the following two procedures, depending on how you backed up the data:

- Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) on page 608
- Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x) on page 609

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:

a. On the Maintenance Web Interface, under **Security**, select **Firewall**.
b. In the Service column, find ping.
c. The checkboxes for both **Input to Server** and **Output from Server** should be checked.

Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release)

Do these tasks ***only*** if you have upgraded from a pre-1.2 release.

To restore translations from a pre-1.2 release:

1. Select **View/Restore Data** under **Data Backup/Restore**.
2. Select **FTP** and enter the information for the FTP backup server.

   Click **View**.
3. Select the Communication Manager translations backup set to restore (filename begins with "xln".

   Click **Restore**.

Important:

Do not restore the system or security backup sets (filenames beginning with "os" and "security"). If you backed up the AUDIX data, you will need to restore the AUDIX backup sets as separate steps. The AUDIX translations, names, and messages backup set filename begins with "audix-tr-name-msg". The AUDIX announcement backup set filename begins with "audix-ann".

To configure the server using the Avaya Installation Wizard

If you have upgraded from a pre-1.2 release (Procedure One), you must enter all server configuration information. You can do this most easily using the Avaya Installation Wizard (IW), which will do the server configuration and install the license and password files. If you have filled in the **Electronic Pre-installation Worksheet (EPW)**, the IW will read the configuration data from the EPW. Otherwise, you will need to enter the configuration data into the IW.

For information on using the Avaya Installation Wizard, see *Job Aid: Avaya Installation Wizard,* 555-245-754. An interactive demo of the IW can be found at http://support.avaya.com/avayaiw.

Restart the server

You must restart the server to capture the configuration data.

1. Telnet to the S8300 and log on.
2. Type **`/opt/ws/drestart 1 4`**.

   You will see the response, `Killed`.

Procedure Two: Restoring data backup (If upgrading from R1.2.x through 2.x)

Do these tasks:

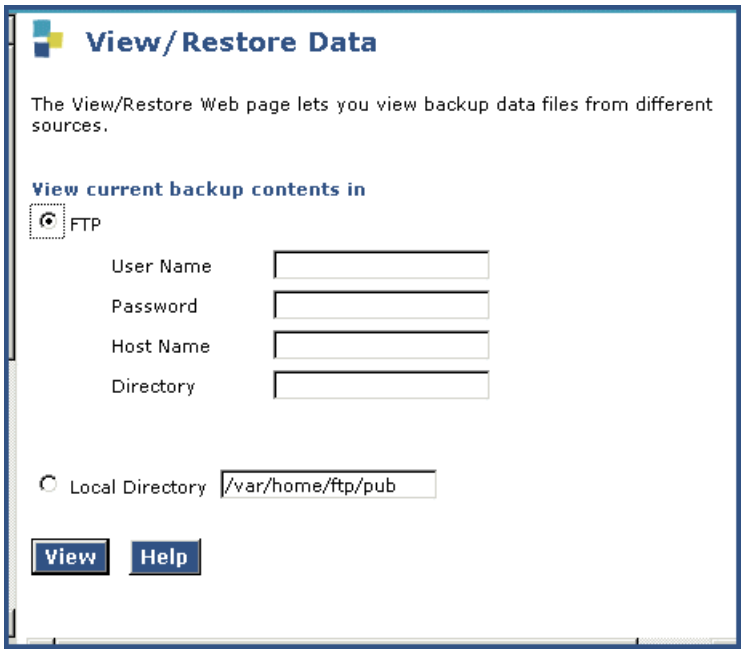
- if the original release was between **1.2.0** and **1.3.9**, and you performed a Linux Migration backup
- or if the original release was **2.0** or later and you performed a normal data backup

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



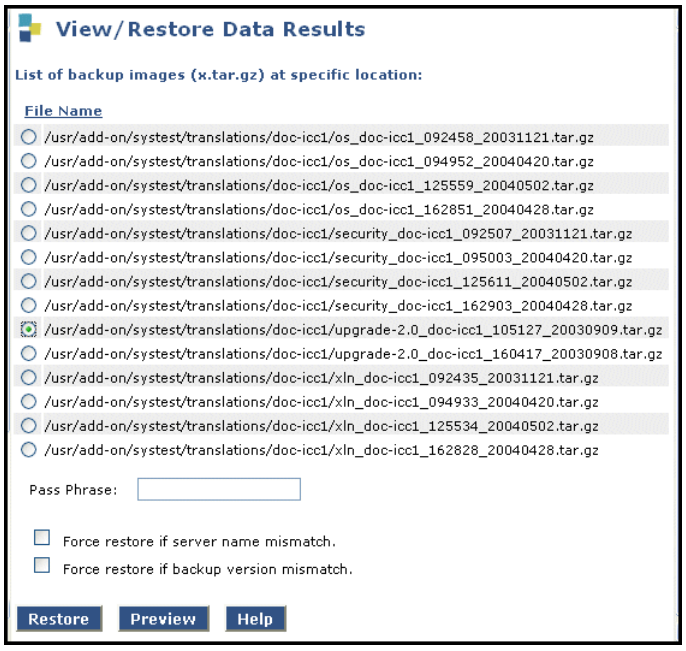
2. Select **FTP**.

   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



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."

   Note that the time and date are embedded in the file name. Select the backup sets with the current time and date stamp.

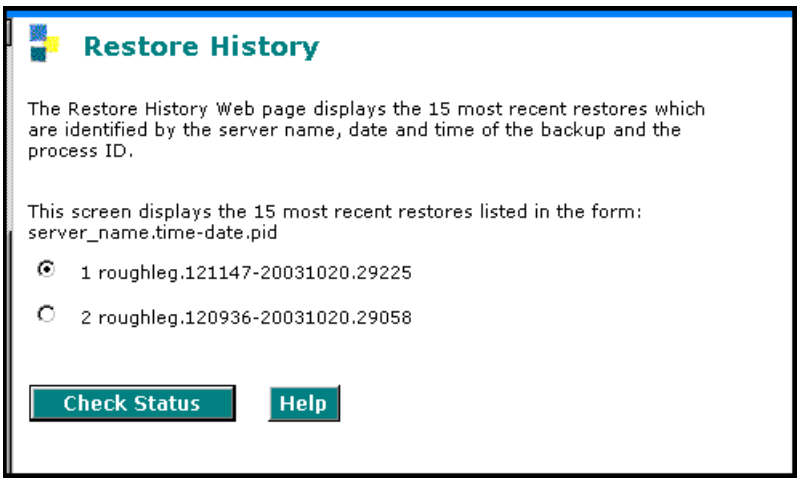
5. Select both **Force** options, and click **Restore**.

6. To monitor the restore progress:

   a. Select **Restore History**

      The **Restore History** screen displays.

Restore History screen



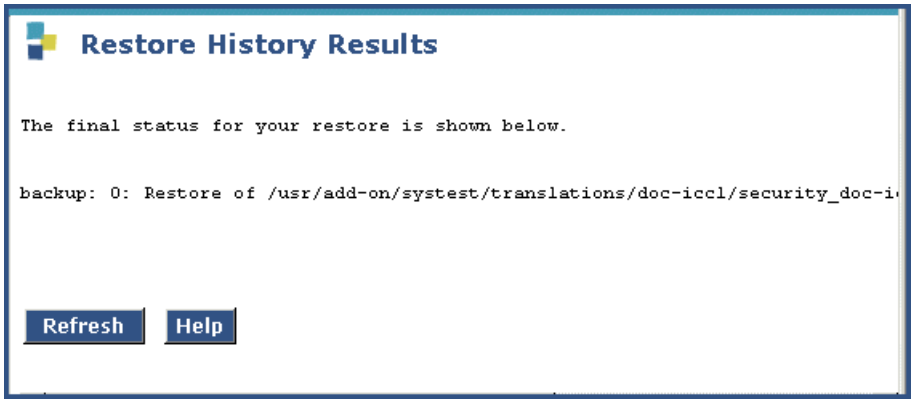
b. Select the backup set being restored and click **Check Status**.

   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



If restoring files from a 2.0.x release, repeat the restore procedure for each backup set, except the AUDIX data (msg and annc files), if any:

- Translations: xln files
- System: os files
- Security: security files

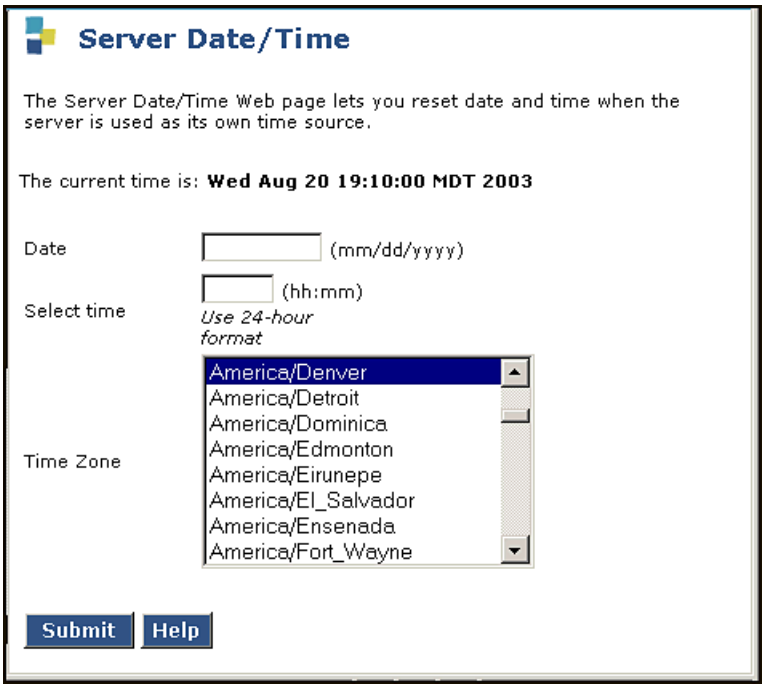
Verifying the time, date, and time zone

To verify the time, date, and time zone

1. Under Server click **Server Date/Time**.

   The **Server Date/Time** screen displays.

Server Date/Time screen



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).

Verifying media server configuration

Note:

If you upgraded from a pre-1.2 release, you should have already completed the server configuration (see Procedure One: Restoring data backup (if upgrading from a Pre-1.2 release) on page 608). In this case, skip to Installing the new license file on page 615.

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. Log on to a Telnet session.
7. Type `/opt/ws/drestart 1 4` to capture the configuration data.

   You should see the response, `Killed`.

Installing the new license file

CAUTION:

Be sure to install the license file ***before*** the authentication file.

You need to load a new license file when upgrading to a new major release of Communication Manager or when changing the feature set.

Note:

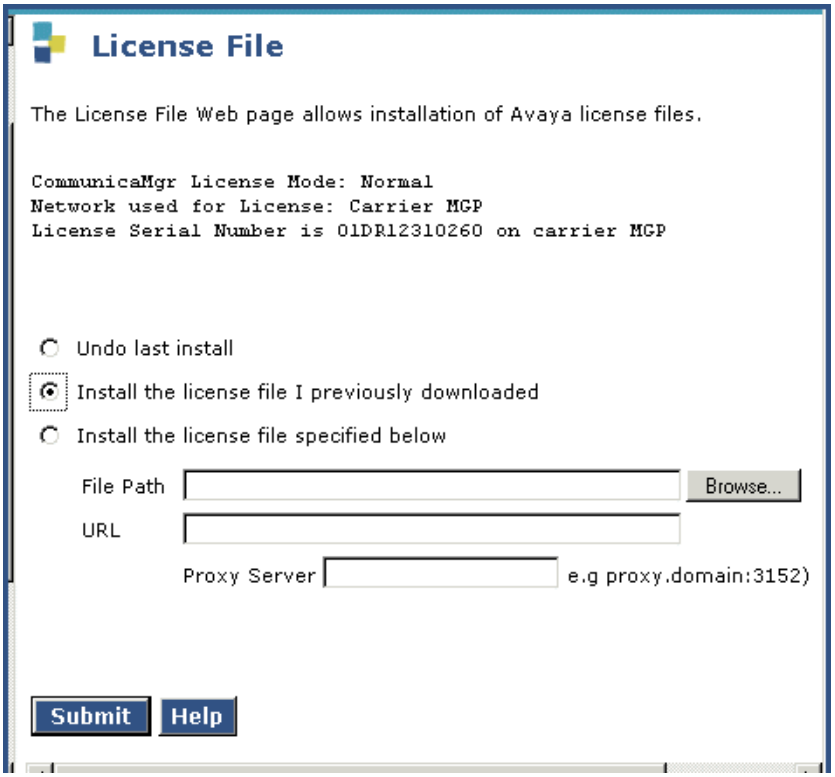
If the S8300 is already set up for remote access, Avaya services personnel can copy new license and authentication files directly into the /pub directory on the server. Avaya personnel will notify you when the new files are in place as agreed (for example, by telephone or E-mail). After they are loaded into the /pub directory, install them using the **License File** and **Authentication File** screens under **Security** on the Maintenance Web Interface.

To install the new license file, if any

1. On the Maintenance Web Interface under **Security**, click **License File**.

   The **License File** screen displays.

License File screen



2. Select **Install the license file I previously downloaded**.

   Browse to the license file on the services laptop, and click **Submit**. The system tells you when the license is installed successfully.

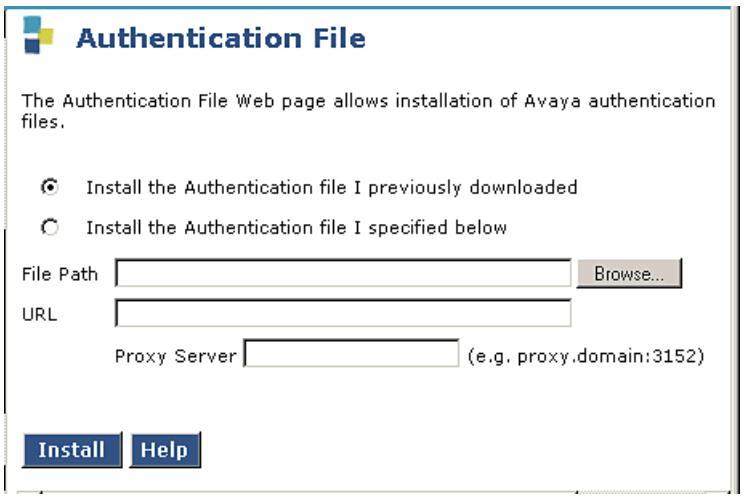
Installing the new authentication file, if any

To install the new authentication file

1. On the Maintenance Web Interface under **Security**, click **Authentication File**.

   The **Authentication File** screen displays.

Authentication File screen



2. Select **Install the Authentication file I previously downloaded**.

   Browse to the authentication file on the services laptop, and click **Install**. The system tells you when the authentication is installed successfully

3. Verify that the restoration of the backup files was successful by testing the *craft* login.

   Telnet to **192.11.13.6** and login as *craft*, using the normal craft password.

   Note:

   If you log into SAT and see the `Translation corruption` message, ignore it for now.

Note:

Avaya Services personnel only: You may need to use the static *craft* password at this point. The 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.

Note:

Avaya Business Partners should call 877-295-0099.

Saving translations (if not using IA770 and S8300 is not an LSP)

Skip this procedure if the S8300 is an ***LSP***, or if ***IA770*** is being used.

CAUTION:

If the system is using IA770, ***do not*** save translations at this time. Skip to Verifying operation on page 617. You will save translations ***after*** installing the new IA770 software.

To save translations (S8300 is not LSP, and IA770 is not used)

1. In a telnet session, open a SAT session.
2. Log in again as *craft*.

   Note:

   If you see the `Translation corruption` message on the first SAT screen, ignore it. Go to Verifying operation on page 617. You will need to save translations later.

3. Type **`save translation`** and press **Enter**.

   When the save is finished, the system displays the message,

   `Command successfully completed.`

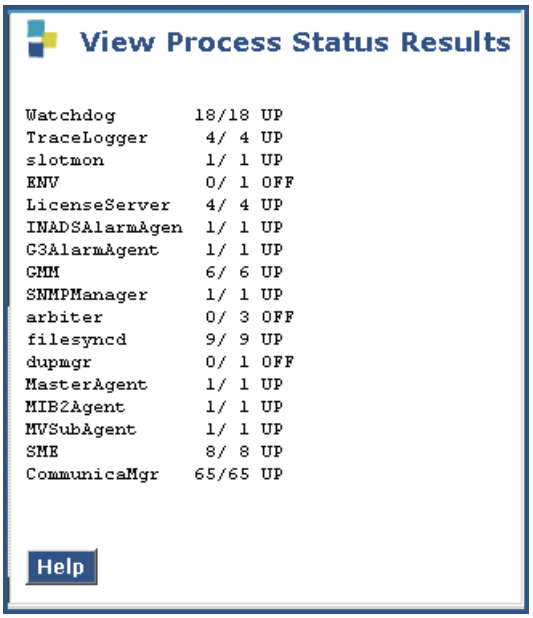
Verifying operation

To verify operation

1. On 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 Results screen



3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**.

   Communication Manager should show **65/65 UP**.

   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.

4. Using a telephone, make test calls to verify that call processing is working.

Next steps

This completes the S8300 upgrade process for upgrading to release 3.0. You now must upgrade the G700 and media module firmware and then install and restart IA770, if installed on the S8300.

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.

This section covers:

- Verifying the contents of the tftpboot directory on page 619
- Determining which firmware to install on the G700 on page 620
- Installing new firmware on the P330 Stack Processor on page 622
- Installing new firmware on the G700 Media Gateway Processor on page 622
- Installing new firmware on the media modules on page 624
- Installing new firmware on other G700 media gateways on page 627

Manually upgrading G700 firmware

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   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.

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

```
FLASH MEMORY    IMAGE VERSION
Bank A          109
Bank B          210

ACTIVE NOW      ACTIVE AFTER REBOOT
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 v*x***

   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).

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

Complete the following tasks after you have finished the upgrade:

If using IA770:

1. Install and restart IA770 on page 629
2. Saving translations on page 635
3. Installing IA770 service pack (or RFU) files and optional language files, if any on page 635

Complete the upgrade process (S8300 is the primary controller):

4. To check media modules on page 636
5. To enable scheduled maintenance on page 636
6. To busy out trunks on page 636
7. To check for translation corruption on page 637
8. To resolve alarms on page 637
9. To re-enable alarm origination on page 637
10. To back up the system on page 637
11. To restart LSPs (if any) on page 637

If using IA770:

Install and restart IA770

To install and restart IA770

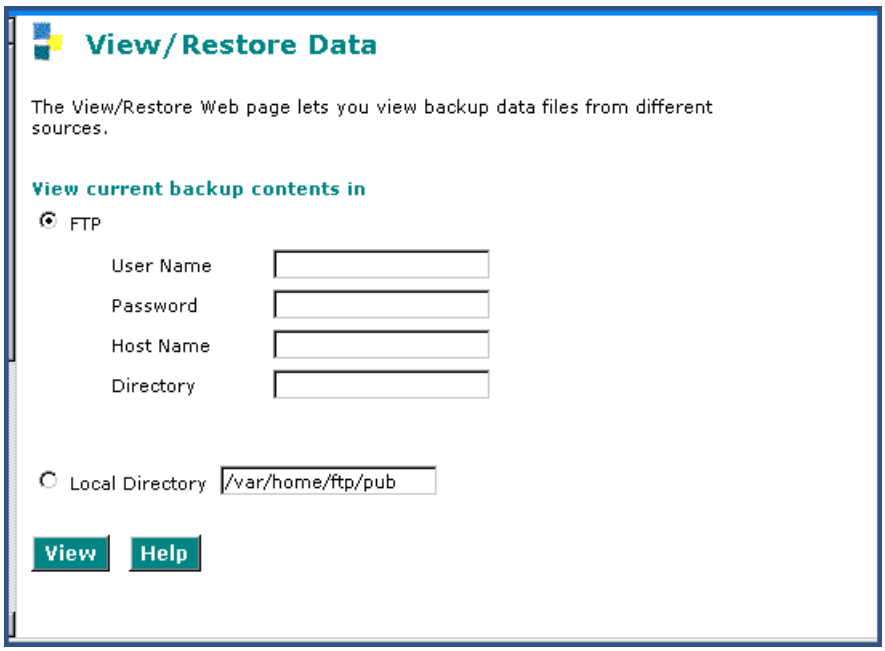
1. Telnet to **192.11.13.6**
2. Log in as **craft** or *dadmin*.
3. Type **cd /usr/CHIA**
4. Install IA770:
   a. Type **sudo ./autoinstall**
   b. When prompted to stop call processing, select **y**.
      The installation should take about 10 minutes from this point.

   Note:
   Communication Manager will shutdown.

   c. Ensure that the autoinstall script completed successfully.
      You will see the message,
      `Successful Completion of IA770 Automatic Installation.`
5. Enable messaging:
   a. Go to the Web Interface and select **Messaging Software** under Miscellaneous.
   b. If the **Enable** button shows at the bottom of the screen, click it to enable messaging.
      If the **Disable** button is showing, messaging is already enabled.

   Note:
   This does not start messaging. Communication Manager and Messaging are still stopped at this point.
6. Restore AUDIX data:
   a. Under Data Backup/Restore, click **View/Restore Data**.
      The **View/Restore Data** screen displays.

View/Restore Data screen



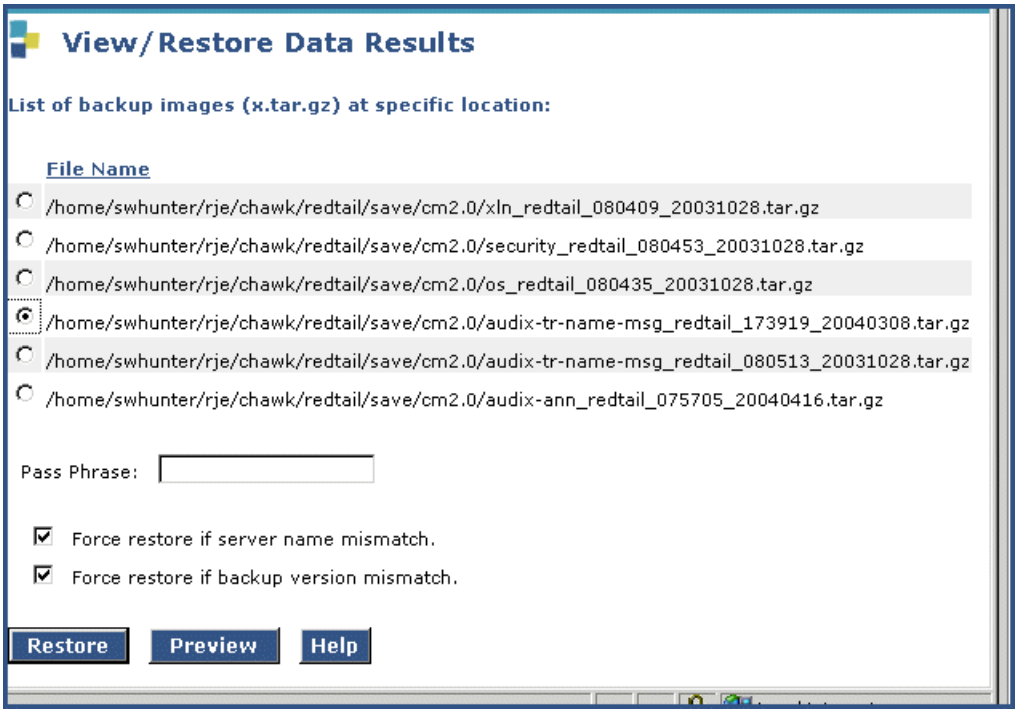
b. Select FTP and enter the information for the location of the backed up **AUDIX Translations**, **Names**, and **Messages** and click **View**.

   The **View/Restore Data Results** screen displays.

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.

View/Restore Data Results screen



c. Select the **AUDIX Translations, Names, and Messages** backup set (that is, the file with **audix-tr-name-msg** in the filename)

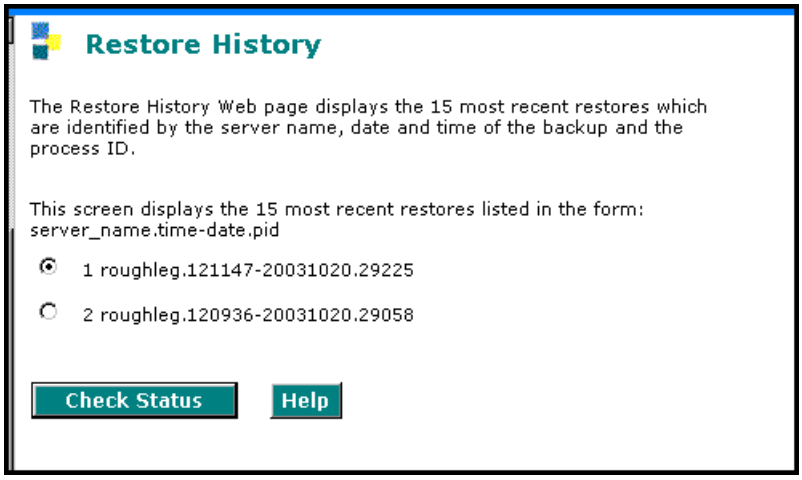
d. Select both **Force** options, and click **Restore**.

To monitor the restore progress

1. Select **Restore History**.

   The **Restore History** screen displays.

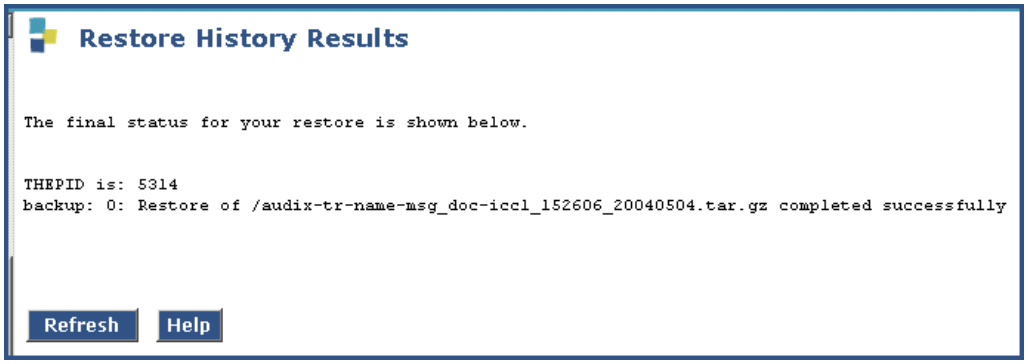
Restore History screen



2. Select the backup set being restored, and click **Check Status**.

   The **Restore History Results** screen displays.

Restore History Results screen



3. Click **Refresh** periodically until the **Completed Successfully** message appears.

   This restore process could take 30 minutes or longer.

   Note:

   Warning messages similar to the message shown on this screen are expected and do not require any action.

To restart Communication Manager

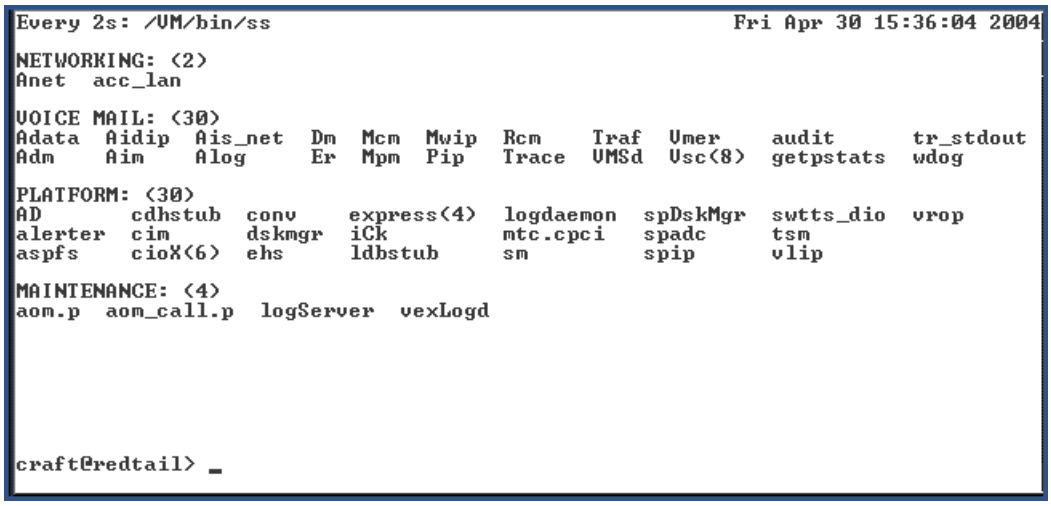
1. Open a Telnet session to the S8300 and type **`start -a`**
2. Ensure that all Communication Manager processes come up.

To monitor the startup of IA770

1. Type **watch /VM/bin/ss**

   The display will periodically refresh automatically. When you see the following display, the IA770 startup is complete.

IA770 startup complete screen



2. Press **Ctrl**+**C** to break out of the **watch** command.

To verify operation

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

3. Make sure everything except **ENV**, **arbiter**, and **dupmgr** shows **UP**. **Communication Manger** 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. 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 telnet 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.`
4. If an IA770 post-upgrade service pack is required, see the IA770 documentation for procedures to install the service pack.

Installing IA770 service pack (or RFU) files and optional language 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.

To obtain the post-upgrade service pack file and documentation

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.
7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 software.

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.
7. To install the language files, under Miscellaneous click **Messaging Administration**, then **Utilities**, then **Software Management**, then **Software Installation**. Follow the instructions to install the language software.

Complete the upgrade process (S8300 is the primary controller)

Telnet to the S8300 (primary controller) and open a SAT session 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 Pre-Upgrade Tasks — If the S8300 is the primary controller on page 578).

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. Open a Telnet session on the S8300 (LSP).
2. At the command prompt, type **start -ac** and press **Enter**.

This completes the upgrade process for a G700 with an S8300.

Chapter 12: Upgrade of an existing S8300B to R3.0 with manual upgrade of G700 firmware

This chapter covers the procedures to upgrade the software on an installed Avaya S8300B Media Server from a 2.x release to 3.0. 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 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware

About upgrading the S8300B to release 3.0 and upgrading G700 firmware

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 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.
- The Upgrade Tool cannot be used on an S8300 configured as an LSP.

CAUTION:

This upgrade procedure requires a service interruption of approximately 2 hours, or up to 4 hours if IA770 is being used.

To upgrade the S8300B to release 3.0, it is necessary to install a pre-upgrade service pack that prepares the server's Web Interface to load the upgrade RPM files from the Server CD onto the S8300 hard drive.

Note:

With release 3.0 of Communication Manager, the Server CD no longer has *.tar or *.tar.gz files. These have been replaced with RPM files that use storage space on the Server CD and the S8300 hard drive more efficiently. To work with these files requires a pre-upgrade service pack installation.

Major tasks to upgrade the S8300B to release 3.0 and upgrade the G700 firmware

The major tasks to upgrade the S8300B to release 3.0 and upgrade the G700 firmware are:

- Before going to the customer site
- On-site Preparation for the Upgrade
- Upgrade the S8300
- Upgrade the G700 Firmware
- 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:

- Planning forms that the project manager provides on page 641
- Getting the serial number of the G700, if necessary on page 641
- Checking the number of allocated ports on page 641
- Checking the FTP server for backing up data on page 641
- Obtaining S8300 software and G700 firmware on page 642
- Obtaining service pack and language files, if using IA770 on page 644
- Completing the RFA process (obtaining license and password file) on page 645

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, passwords, people to contact, the type of system, and 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.

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, 1.3 to 2.0), you will need the serial number of the G700. To get this number, ask the customer's administrator to log in to 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

Release 3.0 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. Ask the customer to check the system for the maximum number of ports. This can be done using the SAT command, **`display system-parameters customer-options`**. Verify that the **Maximum Ports:** field is `900` or less.

Checking the FTP server for backing up data

During the installation and upgrade procedures, you will need to back up the system data to an FTP server. Normally, you will use an FTP server on the customer's LAN for backups.

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

Check with your project manager or the customer for this information.

Important:
Before going to the customer site, make sure that you can use a customer server for backups.

Obtaining S8300 software and G700 firmware

The file containing the software for the S8300 has a ***.tar** extension and contains both the S8300 software and the G700 firmware. The ***.tar** file is on a CD-ROM that you take to the site. This CD is called the “Server CD” because in 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)
- G700 firmware file (most recent version)

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

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 37: 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 3.0. You must escalate.

Table 37: 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.02.0.xxx.x	02.0.xxx.x-xxxx.tar.gz

To download a pre-upgrade service pack

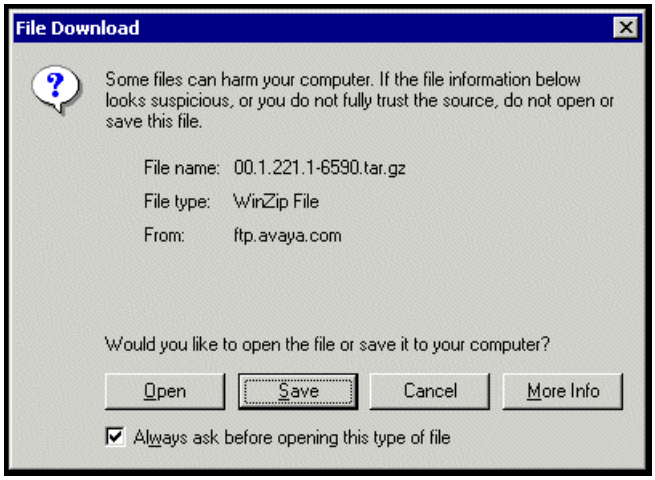
1. On your laptop, create a directory to store the file (for example, c:\S8300download).
2. Connect to the LAN using a browser on your laptop or the customer's PC and access http://www.avaya.com/support on the Internet to copy the required Communication Manager service pack file to the laptop.
3. At 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 3.0**).
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, if using IA770

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 3.0 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 **Messaging** in the list on the left.
2. Scroll down to the INTUITY links and double click on **IA 770 INTUITY AUDIX Messaging Application**.
3. Double click on **All Documents**.
4. 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**.
5. Double click on the service pack file name. For example, **C6039rf+c.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 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, S8500, S8700, S8710, or Blade 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.

On-site Preparation for the Upgrade

Perform the following tasks before starting the software upgrade on the S8300:

- Accessing the S8300 on page 648
- Completing pre-upgrade tasks — If the target S8300 is the primary controller on page 649
- Getting IA770 (AUDIX) Data and Stopping IA770 (if IA770 is being used) on page 652
- Backing up S8300 recovery system files on page 656
- Installing the pre-upgrade software service pack on page 658
- Copying the software and firmware files from the Server CD on page 661

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 48.

You will use both telnet and the Maintenance Web Interface to perform the procedures.

To access the S8300 using telnet

1. Click **Start > Run** to open the **Run** dialog box.
2. Type `telnet 192.11.13.6` and press **Enter**.
3. Log in as *craft* or *dadmin*.

To access the S8300 using the Maintenance Web interface

1. Launch the Web browser.
2. 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**.

To access SAT

1. From the bash CLI, type **SAT** and press **Enter**.

   Or, to open SAT directly from your laptop,

   Click **Start > Run**, type **telnet 192.11.13.6 5023**, and press **Enter**.
2. Log in as *craft* or *dadmin*.

3. Enter **w2ktt** for the **Terminal Type** (if you are running Windows 2000 on your laptop).
4. Accept the default (`y`) for **Suppress Alarm Origination**.

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 666.

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 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 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 (AUDIX) Data and Stopping IA770 (if IA770 is being used)

Skip to Backing up S8300 recovery system files on page 656 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.

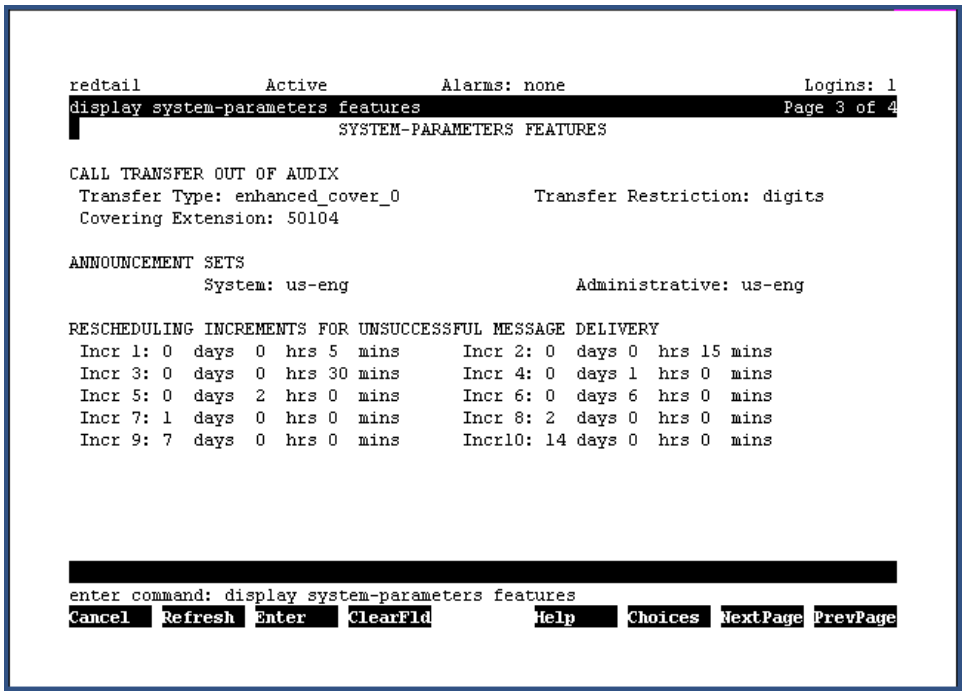
Determining whether optional languages are needed

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



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 Manger 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 655 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

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.

Backing up S8300 recovery system files

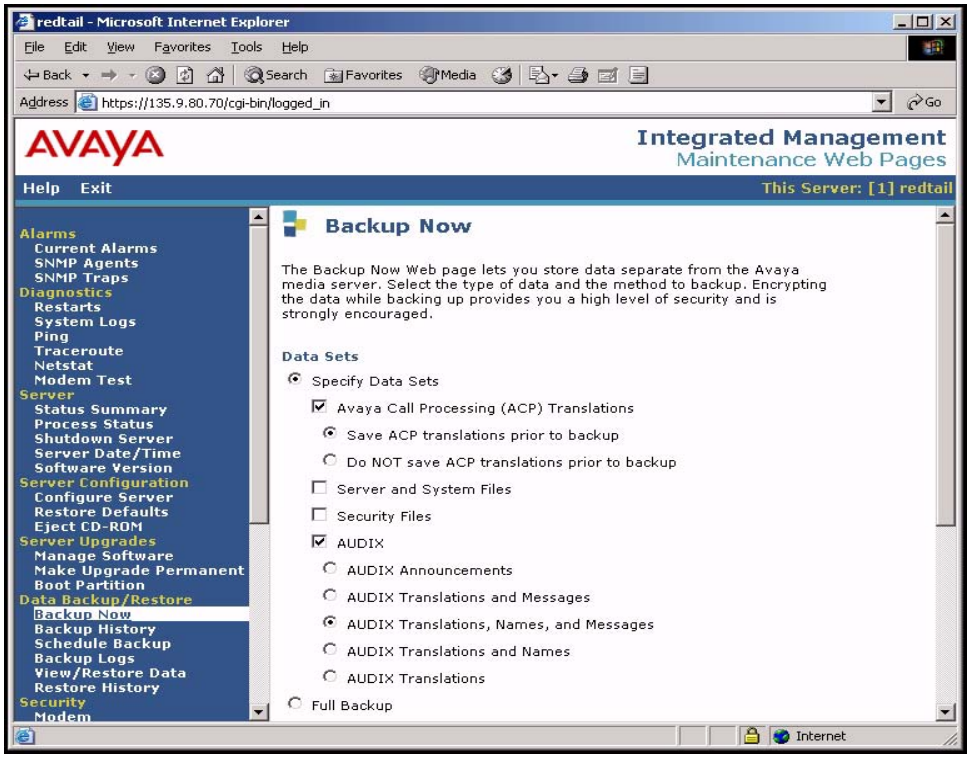
Before installing the S8300 software, back up the system data in case you need to back out of the upgrade. You should back up to an FTP server on the customer's network. To do this, you need an FTP address and directory path and a user ID and password to access the customer's network. Check with your 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 all data sets:
   - Avaya Call Processing (ACP) Translations
   - Save ACP translations prior to backup

   Note:

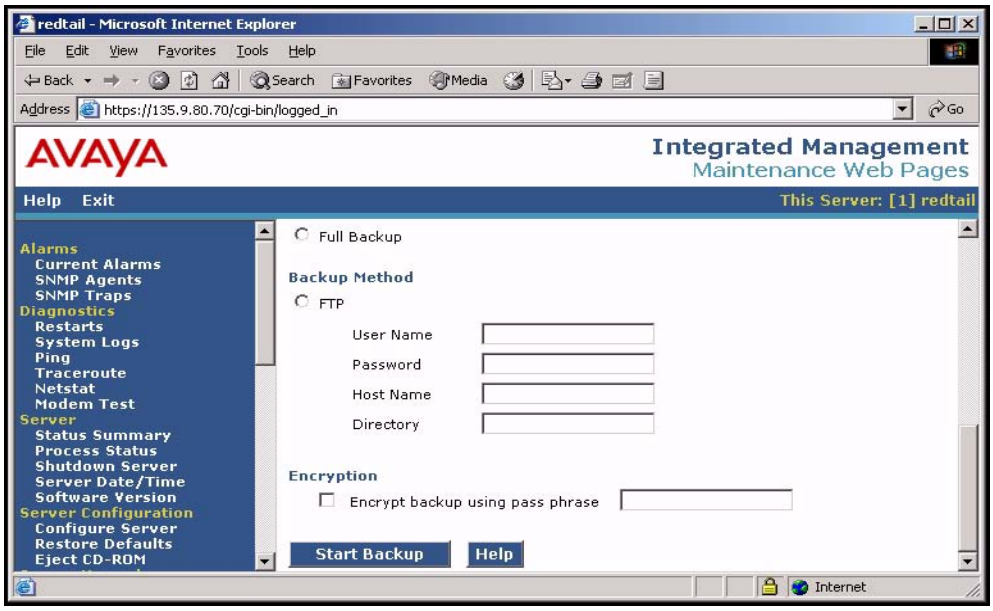
   Select this option only if the S8300 is a primary controller. Do not select it if the S8300 is an LSP.

   - 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.

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.

Installing the pre-upgrade software service pack

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 3.0 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 license and authentication files to the S8300 hard drive (from your laptop)

Skip to Copying the software and firmware files from the Server CD on page 661 if you are not installing a new license or password file.

For an upgrade, you need to install a license file when:

- Upgrading to a new major release of Communication Manager (for example, R2.x to R3.x)
- Changing the feature set

Note:

If the S8300 is already set up for remote access, Avaya services personnel can copy new license and authentication files directly into the FTP directory on the server. Avaya personnel will notify you when the new files are in place as agreed (for example, by telephone or E-mail). After they are loaded into the FTP directory, install them using the **License File** and **Authentication File** screens from the S8300 main menu web-page.

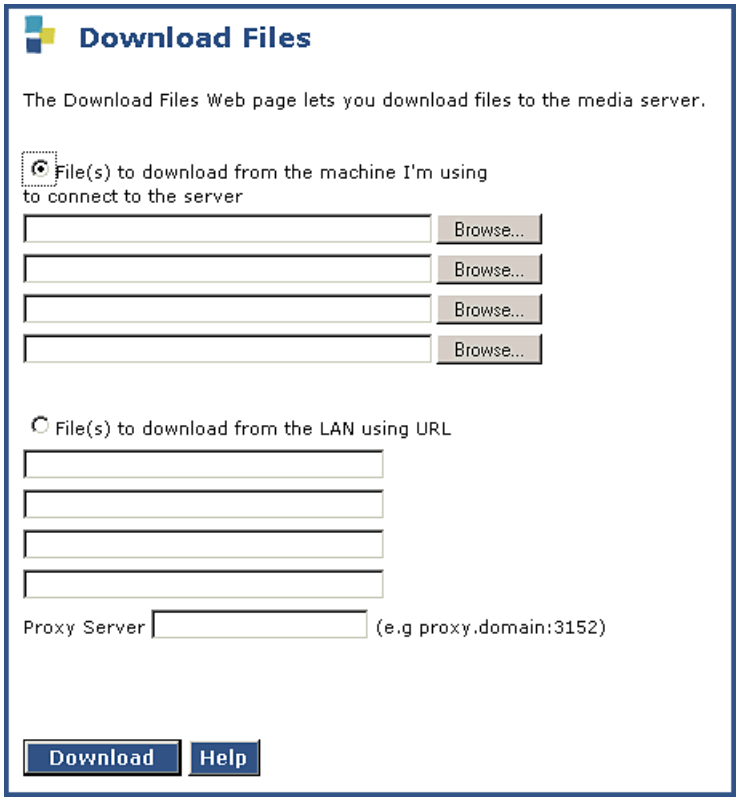
Use the following procedure to transfer the license and password files from the CD or hard drive on your laptop to the S8300 hard drive.

To copy license and authentication files to the S8300 hard drive from your laptop

1. Log on to the S8300 Web Interface
2. In the main menu under Miscellaneous, click **Download Files**.

   The **Download Files** screen displays.

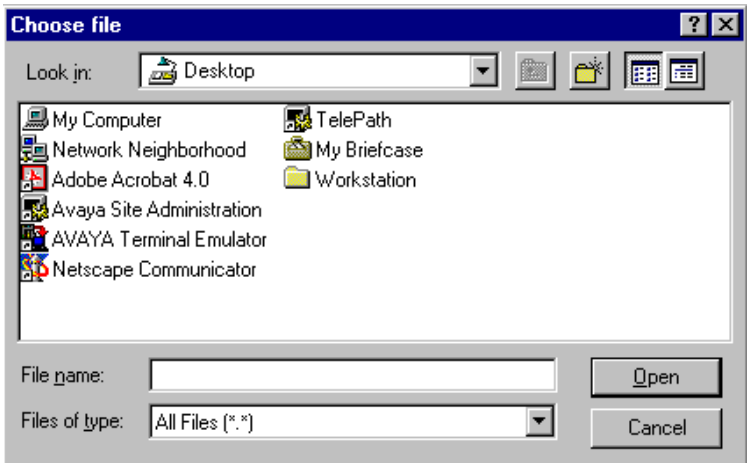
Download Files screen



3. Select **Files to download from the machine I'm using to connect to the server** and click **Browse** for the first field.

   The S8300 displays the **Choose File** screen, which allows you to select files from your laptop.

Choose File Screen



4. Locate the customer's license (**.lic**) file.
5. When you have selected the **.lic** file, click **Open** in the dialog box.
6. Click **Browse** for the second field.
7. Locate the customer's **.pwd** file on your laptop.
8. When you have selected the **.pwd** file, click **Open** in the dialog box.
9. When you have finished entering the files to be copied, click **Download**.

   When the files are successfully transferred, the system displays the status screen.

Copying the software and firmware files from the Server CD

Normally, during an upgrade, you will have the Server 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*, 012-01.0.411.1). The latest service pack software for Communication Manager also reflects the most recent load of software (*for example only*, 01.0.411.1-6592).

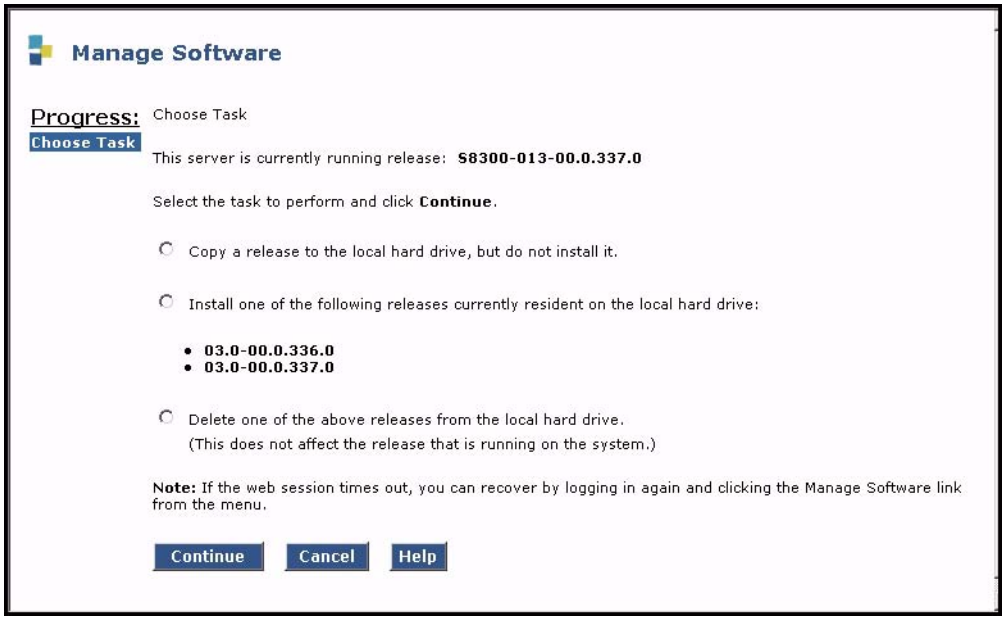
These files also contain the most recent firmware for the G700 Media Gateway, the various media modules, and the P330 Stack Processor.

To transfer files from the Server CD

1. Insert the Server 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



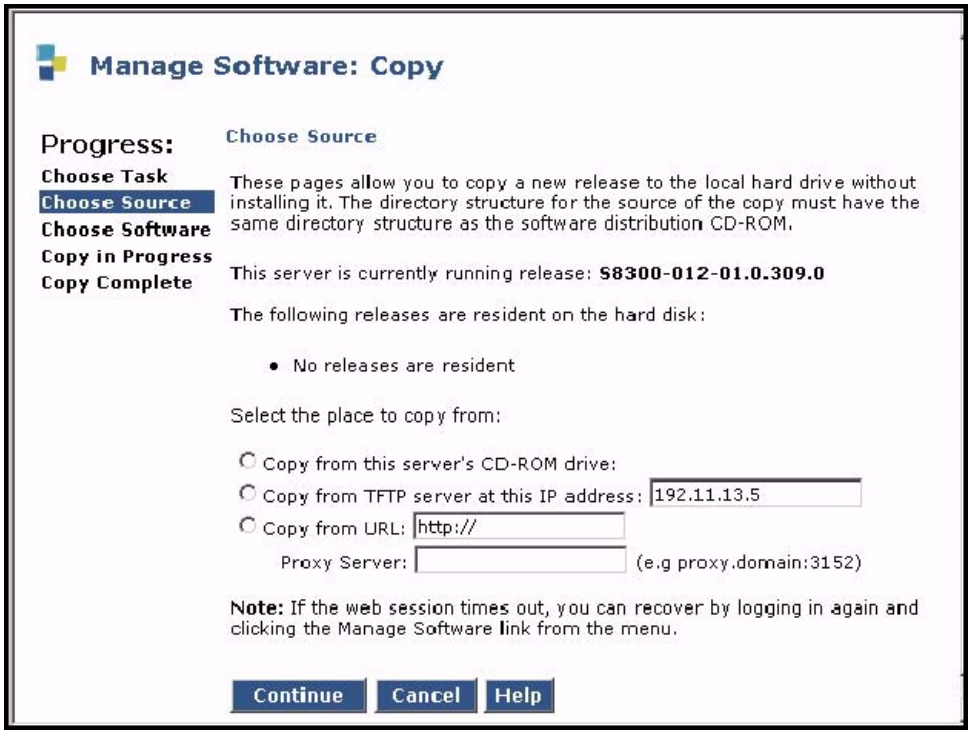
4. Select the radio button **Copy a release to the local hard drive, but do not install it**.

   Note:

   The S8300 hard drive can hold up to three releases without having to delete a release before copying a new release from the Server 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



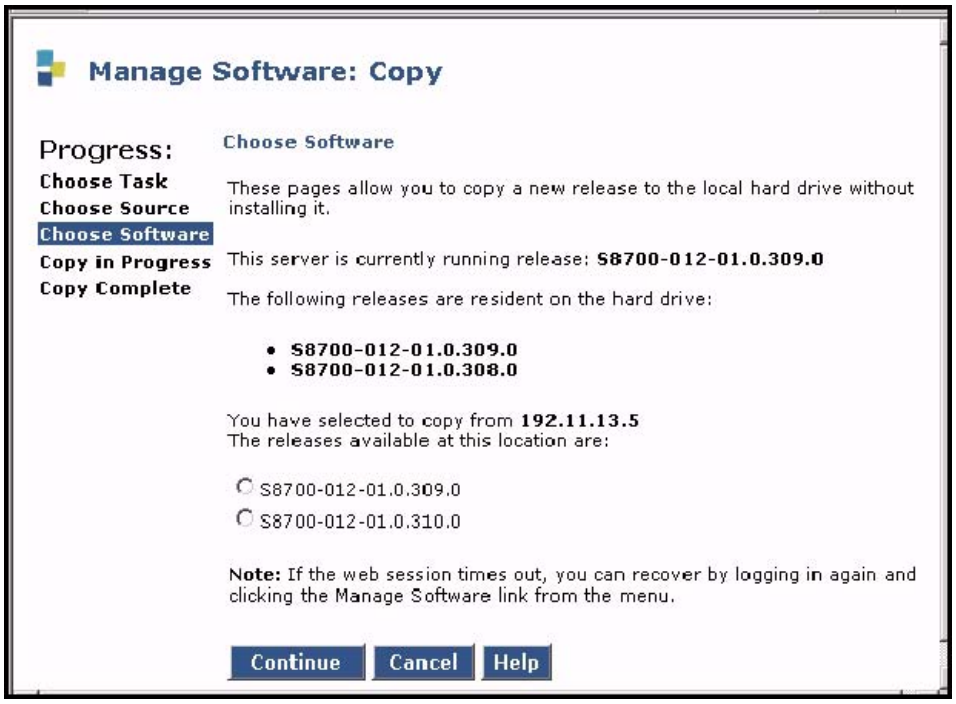
Possible sources include:

- 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.

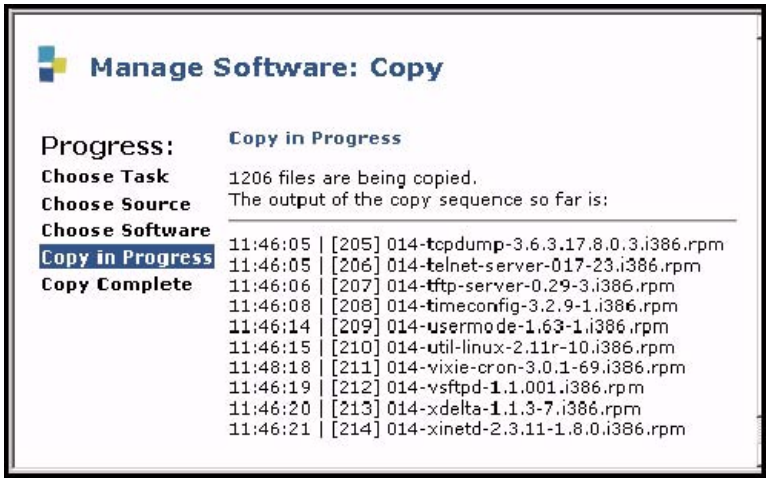
The system displays the **Choose Release** screen.

Choose Release screen



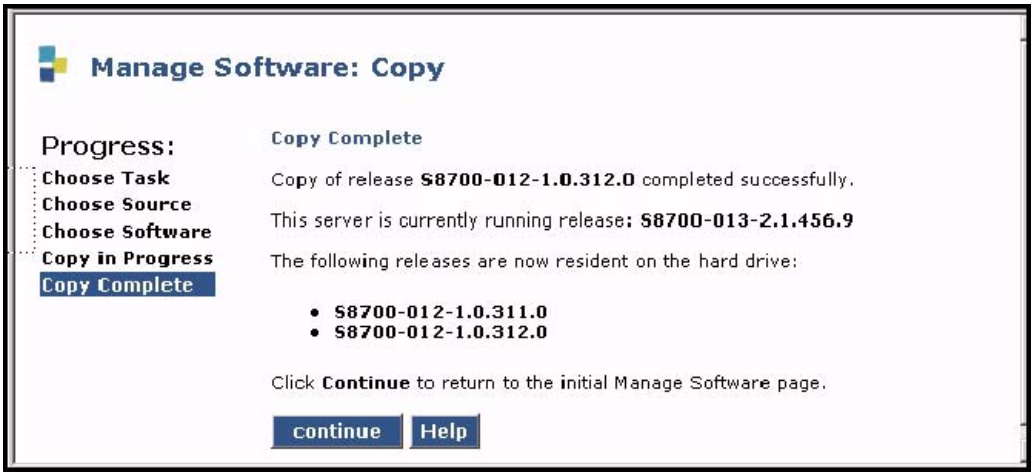
The screen is presented with no radio button selected. The user must select the release to be copied and click **Continue**. The system displays the **Copy in Progress** screen.

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 Media Server from a 2.x release of Communication Manager to release 3.0. To upgrade from a pre-2.0, use the procedures in Chapter 11: Upgrade of an existing S8300A to R3.0 with manual upgrade of G700 firmware.

Manually upgrading the S8300

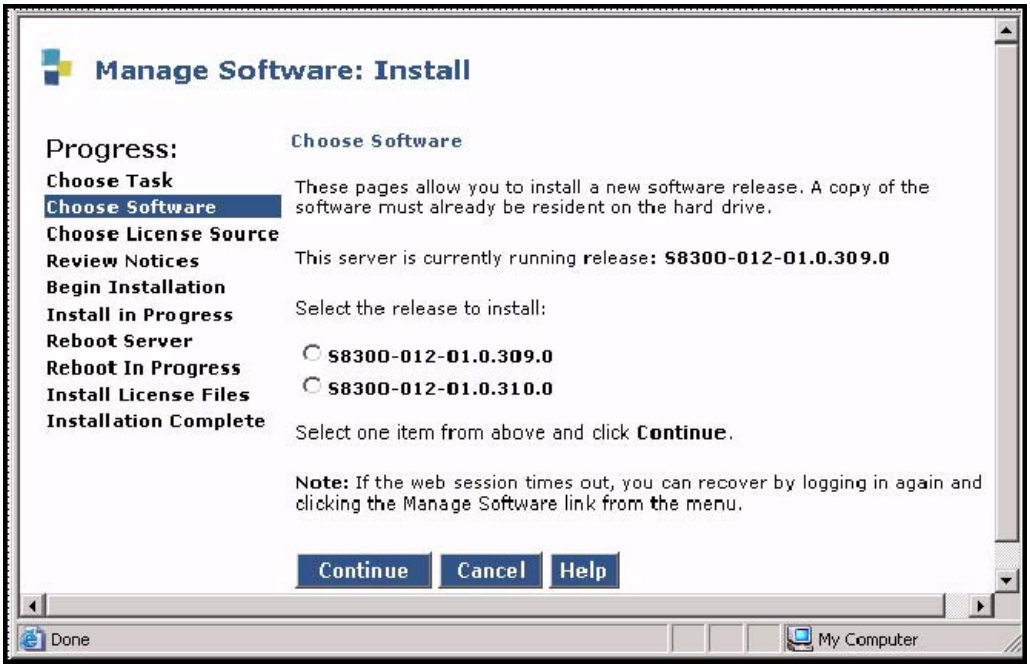
Perform the following tasks to upgrade the S8300 to the most recent load of software:

1. Installing new software on page 666
2. Making the upgrade permanent on page 670
3. Installing post-upgrade Communication Manager service pack file from your laptop, if any on page 671

Installing new software

The first step in upgrading the S8300B Media Server to Communication Manager 3.0 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 from the Server CD on page 661). 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.

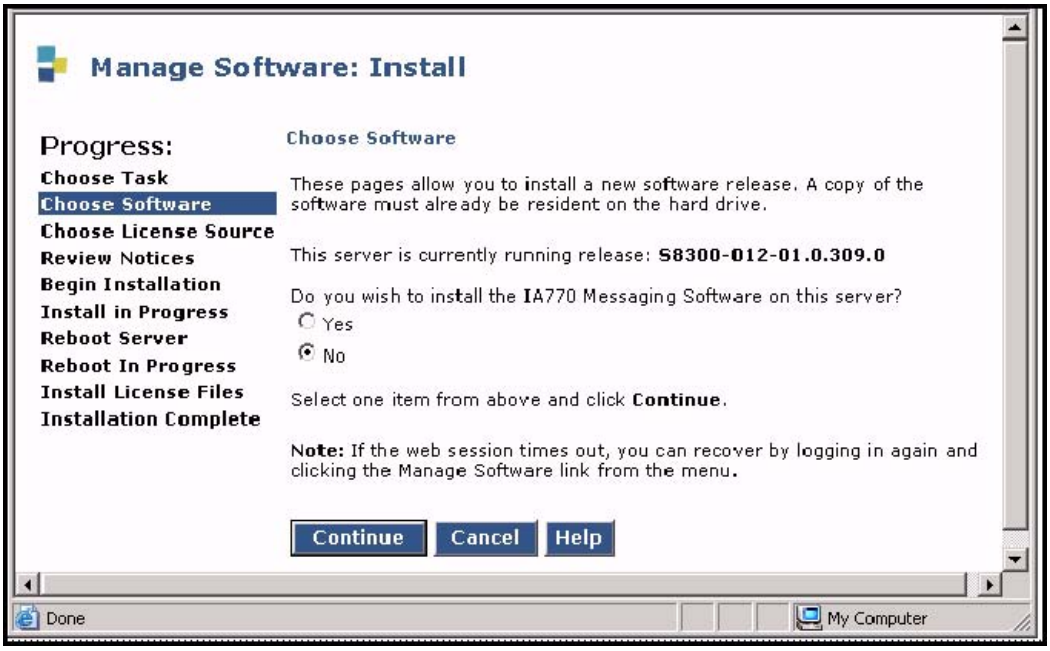
Choose Software screen



This screen will show the release currently running on the S8300B, and the releases resident on the hard drive. To install the 3.0 release, click the radio button next to the 3.0 release and click **Continue**.

The next screen displays in order to support installation of IA770 software.

IA770 Installation Support screen



This screen displays, if and only if:

- IA770 is/is not supported, and
- The server is not an LSP.

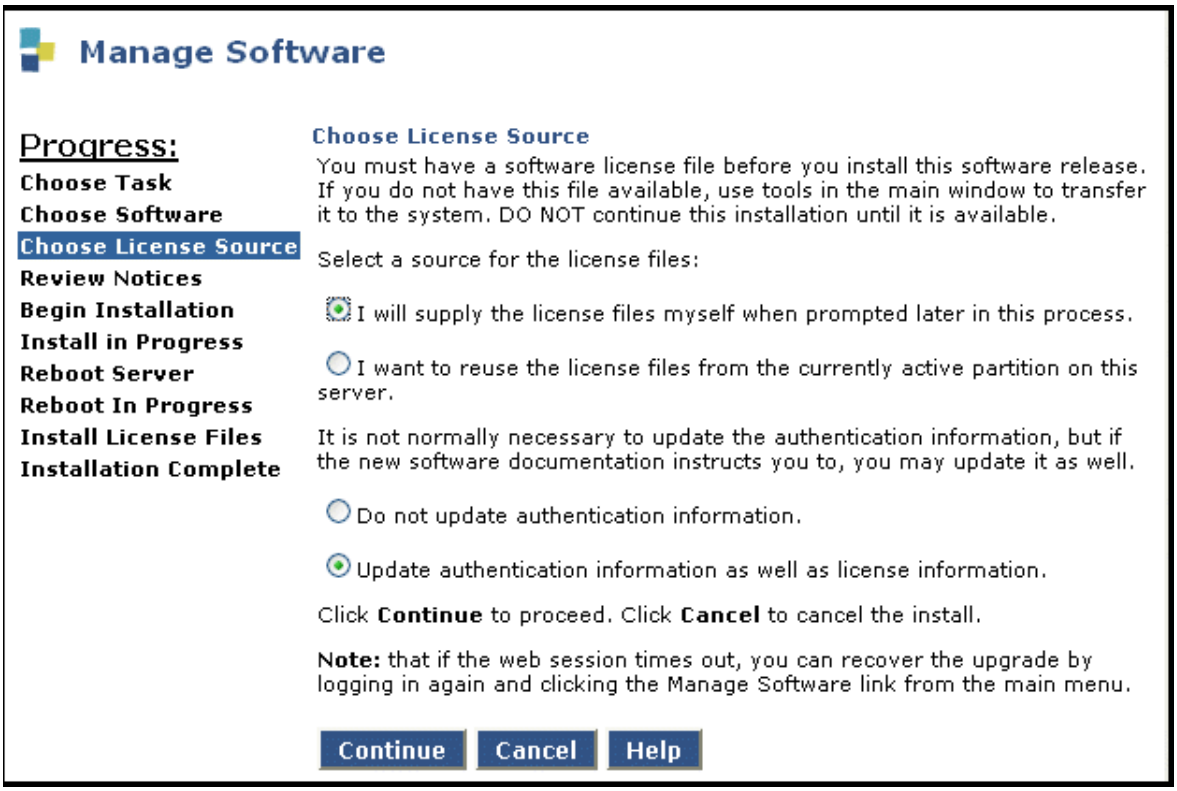
The radio buttons default as follows: If IA770 is not supported, the "no" button will be selected; if IA770 is supported, the "yes" button will be selected.

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



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.

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.

12. Under Server, click **Software Version** to verify the new software version.

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

Installing post-upgrade Communication Manager service pack file from your laptop, if any

Skip to Upgrade the G700 Firmware on page 674 if there is no Communication Manager service pack file to install.

CAUTION:

The service pack may or may not be call-preserving.

To install post-upgrade Communication Manager service pack file from your laptop

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **`telnet 192.11.13.6`** and press **Enter**.
3. Log in with the initial *craft* ID and password. (You cannot use *dadmin* at this point.)
4. Type **`cd /var/home/ftp/pub`** and press **Enter** to access the pub directory.
5. At the prompt, type **`ls -ltr`** and press **`Enter`** to list files in the pub directory.

   The media server displays a list of files in the FTP directory. Verify that the directory contains the Communication Manager **.tar.gz** file you have uploaded, if any.
6. Type **`sudo update_unpack <update>.tar.gz`**, and press **Enter**.

   where **`<update>`** is the release or issue number of the latest service pack file. (For example, **`03.0.219.0-4925.tar.gz`**).
7. Type **`update_show`** and press **Enter** to list Communication Manager files.

   Verify that the new software file was installed.
8. Type **`sudo update_activate <update>`**, and press **Enter**.

   where **`<update>`** is the release or issue number of the latest software file. (For example, **`03.0.219.0-4925`**. Do *not* use the **.tar.gz** extension at the end of the file name).

   The system may initiate a software **`reset system 4`**. You must wait until the restart/reset has completed before entering additional commands.

   If the system displays the message,

   /opt/ecs/sbin/drestart 1 4 command failed

   ignore this message**.**
9. Type **`update_show`** again and press **`Enter`** to list Communication Manager files.

   Verify that the new software file was applied.

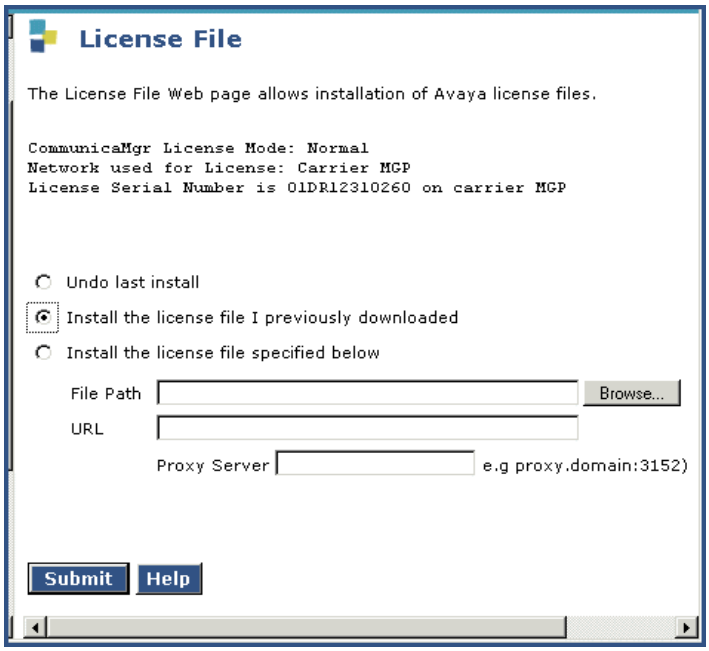
Install updated license and authentication files

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

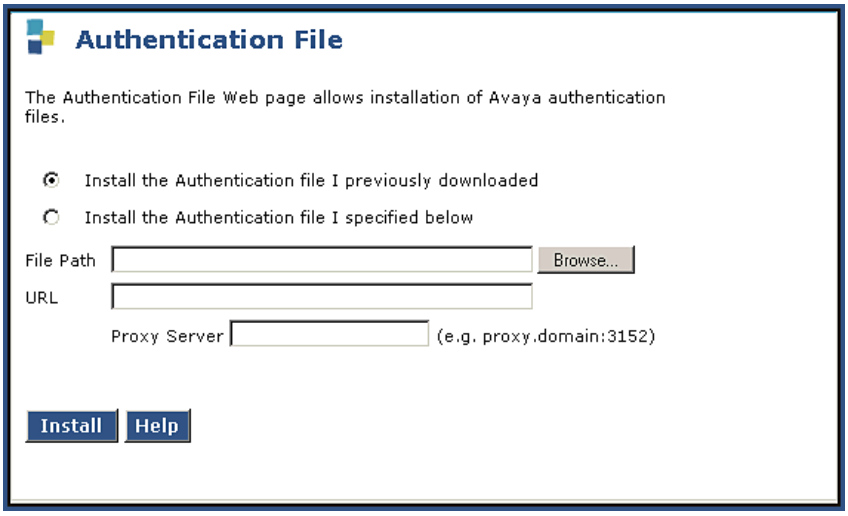


2. Select **Install the license file I previously downloaded** and click **Submit**.

   The system tells you the license is installed successfully.

3. Under Security, select **Authentication File**.
4. The **Authentication File** screen displays.

Authentication File screen



5. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system tells you the authentication file is installed successfully

Saving translations (only if new license and/or authentication files installed)

Skip this procedure if the S8300 is an LSP.

To save translations

1. In the telnet session, open a SAT session. and log in as *craft* (or *dadmin*).
2. At the SAT prompt, type **`save translation`** and press **Enter**.

   When the save is finished, the system displays the message,

   `Command successfully completed.`

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.

Manually upgrading G700 firmware

Conduct the following manual procedures to update the firmware running on the G700 Media Gateway processors and media modules:

G700 Pre-Upgrade Tasks

1. Verifying the contents of the tftpboot directory on page 674
2. Determining which firmware to install on the G700 on page 675

G700 Upgrade Tasks

1. Installing new firmware on the P330 stack processor on page 677
2. Installing new firmware on the G700 Media Gateway Processor on page 677
3. Installing new firmware on the media modules on page 679
4. Installing new firmware on other G700 media gateways on page 682

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   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.

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

```
FLASH MEMORY    IMAGE VERSION
Bank A          109
Bank B          210

ACTIVE NOW      ACTIVE AFTER REBOOT
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 v*x***

   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).

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:

Installing IA770 service pack (or RFU) files, if any on page 683

Completing the upgrade process (S8300 is the primary controller) on page 684

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.

To obtain the post-upgrade service pack file and documentation

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.
7. Under **IA 770 INTUITY AUDIX Messaging Application**, click on **Installation, Migrations, Upgrades & Configurations**.
8. Click on **IA770 INTUITY AUDIX Release 3.0 Installation**.

   This opens the window that contains the document for installing IA770 software.

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 684
2. To enable scheduled maintenance on page 684
3. To busy out trunks on page 684
4. To check for translation corruption on page 684
5. To resolve alarms on page 685
6. To re-enable alarm origination on page 685
7. To back up the system on page 685
8. To restart LSPs (if any) on page 685

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 650).

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.

To restart LSPs (if any)

To restart Communication Manager on an LSP after the upgrade:

1. Open a Telnet session on the S8300 (LSP).
2. At the command line, type **`start -ac`** and press **Enter**.

This completes the upgrade process for a G700 with an S8300.

Chapter 13: Manual upgrade of an existing G700 without an S8300

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 Manger. 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 47 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 689
- Getting the serial number of the G700, if necessary on page 689
- Setting up the TFTP server on your laptop or on a customer PC, if necessary on page 690
- Downloading G700 firmware files to your TFTP directory on page 690

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.

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, 1.3 to 2.1), you will need the serial number of the G700.

To get the G700 serial number

1. Ask the customer's administrator to log in to the S8300 Web page.
2. 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.

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 38:

   Note:

   The latest firmware versions may different from those listed in Table 38. 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.

Table 38: Firmware file formats

Component	Firmware Version Format	Example
P330 Stack Processor	viisa<version id>	viisa4_0_17.exe
P330 Stack Processor	p330<version id>	p330Tweb.4.0.4.exe
G700 Media Gateway	mgp<version id>	mgp_21_16_0.bin
VoIP Media Module and Motherboard VoIP	mm760<version id>	mm760v43.fdl
8-port DCP Media Module	mm712<version id>	mm712v5.fdl
24-Port DCP Media Module	mm717<version id>	mm717v2.fdl
8-port/trunk Analog Media Module	mm711<version id>	mm711h20v60.fdl
4-station/4-CO trunk Analog Media Module	mm714<version id>	mm714v60.fdl
T1/E1 Media Module	mm710<version id>	mm710v9.fdl
8-port BRI Media Module	mm720<version id>	mm720v4.fdl
2-port BRI Media Module	mm722<version id>	mm722v2.fdl

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.

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 692
- Verifying the contents of the tftpboot directory on page 692

as described in this section.

Accessing the P330 stack processor

See About connection and login methods on page 47 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   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.

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 696
- Installing new firmware on the G700 Media Gateway Processor on page 696
- Installing new firmware on the media modules on page 698

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

```
FLASH MEMORY    IMAGE VERSION
Bank A          109
Bank B          210

ACTIVE NOW      ACTIVE AFTER REBOOT
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).

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 Guide for Avaya Communication Manager*, 555-245-207.

Avaya G700 Media Gateway Technical Specifications

Table 39: Technical Specifications provides detailed information on the physical dimensions and tolerances of the G700 Media Gateway.

Table 39: 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 39: 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	5% to 95% non-condensing
Altitude	
Recommended	up to 10,000 feet or 3,000 meters

2 of 2

Cabling Equipment

Table 40: 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 40: 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 40: 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
`set interface inband`	***vlan***	1
	IP address	
	netmask	
`set ip route`	***destination IP address***	
	gateway IP address	
`set time protocol`	***sntp-protocol*** | ***time-protocol***	
`set time server`	***IP address of time server***	
`set timezone`	***zone name***	
	- ***<hours>*** (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`	***vlan***	1
	IP address	
	netmask	
	gateway IP address	
`set hostname`	***hostname***	
`set ip route`	***destination IP address***	
	gateway IP address	
`set mgc list`	***IP address***	
	IP address	
	IP address	
	IP address	
`show system`	***serial number***	

Set Up for VoiP Resources

G700 Media Gateway #

Command	Requested Field	Information to be Entered
`set interface voip`	***number***	V0 for resident VoIP resource of the G700
	ip address	
	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
`set interface voip`	***number***	V0 for resident VoIP resource of the G700
	ip address	
	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 P330 switch #

v1	v2
	v3
Expansion Module	v4

Media Gateway (module) #
or P330 switch #

v1	v2
	v3
Expansion Module	v4

Media Gateway (module) #
or P330 switch #

v1	v2
	v3
Expansion Module	v4

Media Gateway (module) #
or P330 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 41: 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
700316326	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 41: 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 42: 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 43: 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 44: Equipment List: Media Modules

Media Modules

MM710 T1/E1 Media Module	Comcode (for Services Ordering Only): 700315567

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

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.

Table 44: Equipment List: Media Modules (continued)

Media Modules

MM711 Analog Media Module	Comcode (for Services Ordering Only): 700277379
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.	
MM714 Analog Media Module	Comcode (for Services Ordering Only): 700277379
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".	
MM712 DCP Media Module	Comcode (for Services Ordering Only): 700315583
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.	
MM717 24 port DCP Media Module	Comcode (for Services Ordering Only): 700302433
The MM717 DCP Medial 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. **NOTE**: ***No more than 3*** MM717 Media Modules can be installed in a single G700.	

2 of 4

Table 44: Equipment List: Media Modules (continued)

Media Modules

MM720 BRI Media Module	Comcode (for Services Ordering Only): 700315591
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.	

MM722 2-port BRI Media Module	Comcode (for Services Ordering Only): 700277361
The MM722 BRI Media Module supports two BRI ports.	

Table 44: Equipment List: Media Modules (continued)

Media Modules	
MM760 VoIP Media Module	Comcode (for Services Ordering Only): 700315609
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 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”.	

Table 45: Avaya P330 Equipment

Avaya P330 Equipment	
Avaya P330 Stacking Sub-Module (optional)	
Material Code: 108562943	P330 MOD P330 STACKING

CASCADE CABLES	
Material code: 108592445	Avaya P330 CABLE OCTAPLANE STACKING 1FT
Material code: 108592437	Avaya P330 CABLE OCTAPLANE STACKING 6FT
Material code: 108563453	Avaya CABLE ASSY X330RC REDUN STACKING

EXPANSION MODULES

Table 45: Avaya P330 Equipment (continued)

Avaya P330 Equipment		
Material code: 108562927	Avaya MOD P330 1000BSX UPLINK 2PT	The X330-S2 provides 1000Base-SX connectivity with two Multimode Fiber ports (up to 550 m,1804 ft) with LAG and Load Sharing
Material code: 108563032	Avaya MOD P330 1000BLX UPLINK 2PT	The X330-L2 provides 1000Base-LX connectivity with two Single Mode Fiber ports (up to 5 km,3.11 miles) with Link Aggregation (LAG) and Load Sharing
Material code: 108562992	Avaya MOD P330 1000BSX UPLINK 1PT	The X330-S1 provides 1000Base-SX connectivity with one Multimode Fiber port (up to 550 m,1804 ft)
Material code: 108562976	Avaya MOD P330 1000BLX UPLINK 1PT	The X330-L1 provides 1000Base-LX connectivity with one Single Mode Fiber port (up to 5 km,3.11 miles)
Material code: 108562968	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.
Material code: 108562950	Avaya MOD P330 100FX UPLINK 2PT	The X330-F2 adds two 100Base-FX ports which can be aggregated using LAG to provide a 200 Mbps link for backbone or high-speed server applications.

2 of 3

Table 45: Avaya P330 Equipment (continued)

Avaya P330 Equipment

Material code: 108659178	Avaya P330 MOD EXP GBIC 2PT	The X330-G2 provides GBIC connectivity with an adapter for standard GBIC transceivers.
Material code: 700214612	Avaya X330 WAN-2DS1	The X330 WAN-2DS1 provides two T1/E1 ports and a 10/100BaseT port.
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.
Material code: 700247588	V.35 DTE Cable	Used with the X330 WAN-2USP.
Material code: 108659194	Avaya MOD DUAL SPEED OC12/0C3 SMF 15KM	
Material code: 108659186	Avaya MOD DUAL SPEED OC12 OC3 MMF 500M	

3 of 3

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 Server 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

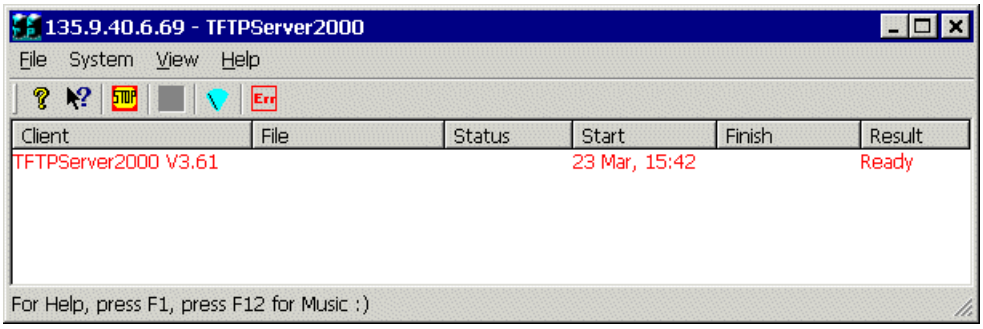
   > Software Downloads

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.

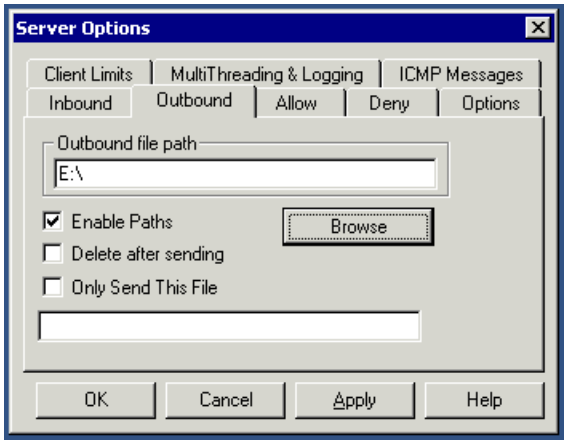
Install the TFTP software

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.

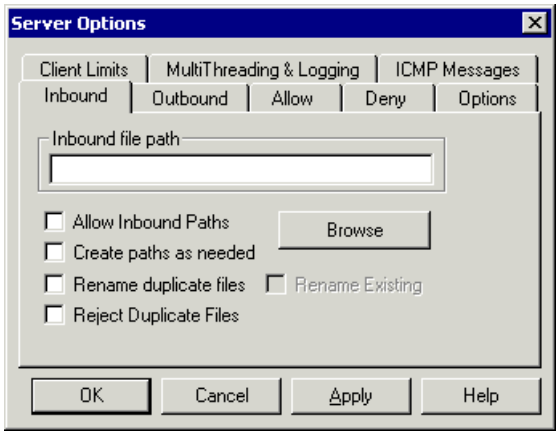
   The TFTP Server window appears.The IP address of the PC plus port 69 shows in the top border.



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



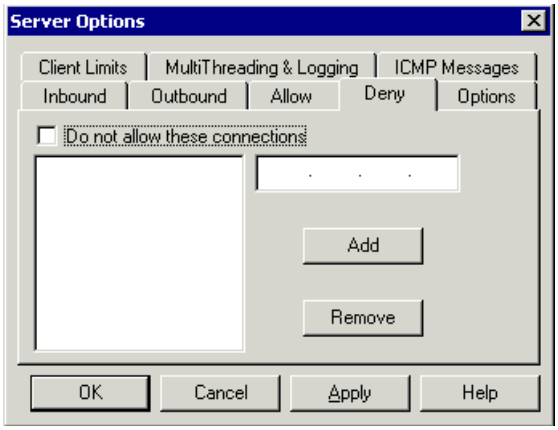
d. Select the **Options** tab. Enter **69** in the **Use Port** field and **30** in the **Timeout** field.

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**.

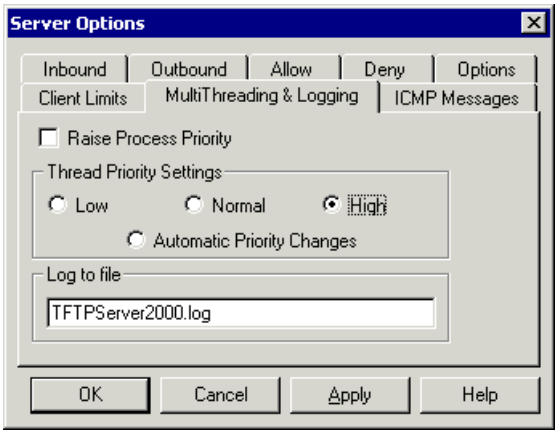
g. In the **Allow** tab, leave the **Only allow these connections** checkbox unchecked.

h. Select the **Deny** tab and ensure that all fields are blank.

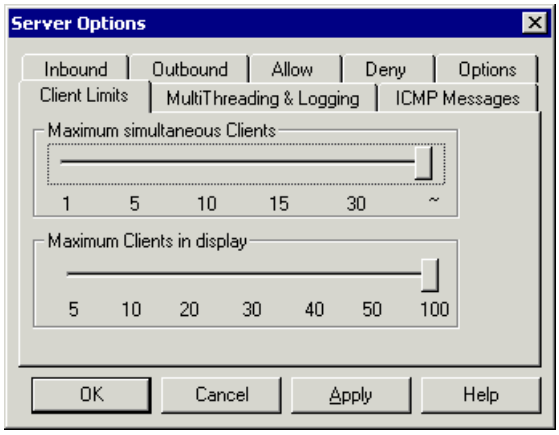


i. Select the **MultiThreading & Logging** tab and select **High** for **Thread Priority Settings**.

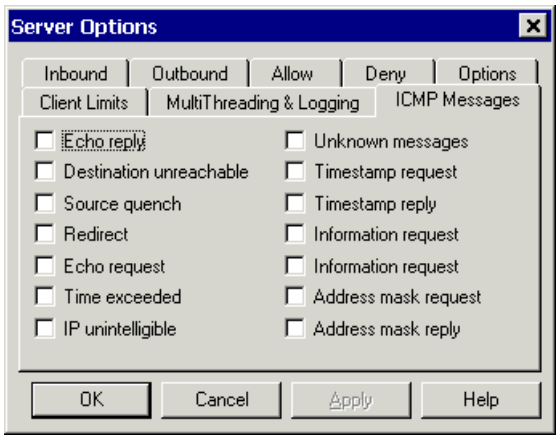
j. Leave the default filename in the **Log to file** field.



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.

Index

Numerical

1151A1 and 1151A2 power supply 347, 349
1151A1 power supply 347
1151A2 power supply 347
120A ICSU 398
2-wire digital station
  connecting 335
  pinout chart 336
  wiring 335
400B2 Adapter 341
4600 Series IP Telephones 335

A

AC power 107
activate pre-upgrade service pack. . 239, 299, 591, 659
adding
  switch configuration 69
adjunct power connections 342
Adjuncts
  connecting 333
alarm wiring 335
analog station
  connecting 335
  wiring 335
announcements 367
approved grounds 104
ART, Automatic Registration Tool 135, 222, 287, 445, 574, 647
ASAI Co-Resident DLG 364
ATM WAN Survivable Processor Manager. 369
Attendant Console, Aux power 342
AUDIX
  IA 770 362
  LX 364
Avaya C360 351
Avaya C460 355
Avaya Site Administration 69, 372
  adding new switch configuration 69
  configuring 69

B

backup
  to FTP server. 216, 568
  to laptop 216, 568
backup, Linux Migration 240, 592
bonding conductor, install 360
BRI stations
  connecting 337
busy tone disconnect 413

C

C460 355
cabling
  multiple units 99
  Octaplane Cables 99, 701
Call Center. 366
  G700 announcements 367
CBC 360
CD, Unity 127, 436
Checklist 1, Install new G700 with S8300 . . . 114, 424
Checklist 2, Install new G700 without S8300 . . 117, 427
Checklist 3, Upgrade G700 with S8300 119, 121, 429, 431
Checklist 4, Upgrade G700 without S8300 . . . 123, 433
checklists 84
Circuit Protection
  Media Modules 361
circuit protection, install 361
CLI commands 71
CO trunk wiring. 335
Command Line Interface Help 66, 67
Configuration Manager 371
configure
  G700 Media Gateway 146, 476
  G700 with S8300 125
    administer Communication Manager. . . 160, 494
    completing installation 179, 515
    G700 serial number 131, 187, 216, 281, 325, 441, 524, 568, 641, 689
    IP connectivity 481, 531
    LSP transition points 484, 534
    manual procedures. 435
    SNMP alarming setup 511
  G700 with S8700 183
    administer Communication Manager 193, 198, 545, 550
    completing installation 181, 209, 517, 561
    Expansion Module 158, 191, 484, 535
    G700 firmware installation 539
    tar.gz file 189, 326, 524, 690
    TFTP server setup 188, 326, 524, 690
  G700 without S8300
    manual procedures. 519
configuring
  Avaya Site Administration 69
  switches 69

connect AC power . . . 109
Connecting
BRI stations . . . 337
connecting a printer to a G700 or G350 Media Gateway . . . 395
Connecting devices
BRI stations . . . 337
consoles
connectable . . . 334
controller list for G700 . . . 482, 532
Co-Resident DLG . . . 364
administration tasks . . . 365
ethernet interfaces . . . 366
coupled bonding conductor, install . . . 360
Customization Template for Avaya Installation Wizard . . . 45
CWY1 Board . . . 363

D

Data Expansion Modules . . . 78
DC
wiring diagram . . . 111
DC power . . . 110
default for media gateway . . . 480, 530
DEFINITY LAN Gateway . . . 364
DHCP server . . . 177, 510
DID trunk wiring . . . 335
Directory Enabled Management . . . 370
DLG . . . 364
DS1 loopback jack . . . 396
DS1 span . . . 397
T1 . . . 396

E

Equipment List
Avaya Expansion Modules . . . 721
G700 . . . 715
Loopback Jack . . . 718
MM710 T1/E1 media module . . . 718
MM711 analog media module . . . 719
MM712 DCP media module . . . 719
MM714 analog media module . . . 719
MM717 DCP media module . . . 719
MM720 BRI media module . . . 720
MM722 BRI media module . . . 720
MM760 VoIP media module . . . 721
Octaplane Cables . . . 721
Power Cords . . . 716
S8300 . . . 717
X330STK Stacking Sub Module . . . 721
Expansion Module
G700 with S8700 . . . 158, 191, 484, 535
installation . . . 97
external alarm wiring . . . 335
external communications controller (ECC) . . . 414

F

Fault and Performance Manager . . . 371
FTP server . . . 216, 568

G

G350 firmware upgrade . . . 268, 314, 331
G600 Media Gateway . . . 83
G700 Media Gateway
rack mounting . . . 90
SNMP alarming setup . . . 511
Gateway Installation Wizard . . . 46
grounding
approved . . . 104
conductors . . . 103
connections . . . 106
requirements . . . 103
safety . . . 106

I

IA770
language files . . . 219, 230, 571, 582
patch files . . . 219, 571
Initial Administration Tasks 161, 166, 193, 198, 495, 500, 545, 550
inserting
Expansion Module . . . 97
X330STK Stacking Sub-Module . . . 98
install
license file . . . 264, 615
installation
checklists . . . 84
roadmap . . . 114, 424
Installation Wizard
Customization Template . . . 45
Electronic Pre-Installation Worksheet . . . 44
gateway installation . . . 46
Names/Number Template . . . 44
installing
telephone power supplies
procedures . . . 339
Integrated Management . . . 369
internal communications controller (ICC) . . . 414
Intuity AUDIX
hunt group . . . 363
IA 770 . . . 362
LX . . . 364
IOLAN+ 104 terminal server . . . 376
installation and administration . . . 376

IP phones
LSP configuration . . . 177, 510
IP route . . . 477, 480, 528, 530
IP services . . . 388
IP Telephone file . . . 253, 455, 604
IP Telephones . . . 335
ISDN BRI stations
connecting . . . 337

K

keys.install file . . . 473

L

LAN switches
C360 . . . 351
C460 . . . 355
languages, for IA770 announcements 219, 221, 230, 276, 284, 285, 292, 294, 571, 573, 582, 635, 644, 645, 652, 654
laptop
as FTP server . . . 216, 568
direct Ethernet connection . . . 158, 191, 484, 535
LEDs . . . 81
license file
install . . . 264, 615
Linux Migration backup . . . 240, 592
Local Survivable Processor . . . 83
loopback jack . . . 396
administration . . . 398
installation . . . 396
LSP . . . 83
IP phones . . . 177, 510
transition of control . . . 178, 511
LSP/G700 Upgrade Tool . . . 45

M

Media Modules . . . 76
Messaging
IA770 . . . 362
LX . . . 364
MM720 media module
connecting ISDN BRI stations to . . . 337
modems, external . . . 411
administration . . . 412
hardware to configure . . . 411
Multi-Tech MT5634ZBA-USB . . . 411
Multi-Tech MT5634ZBA-V92 . . . 412
multiple units . . . 99
MultiService Network Manager . . . 370
MultiService SMON Manager . . . 371
Multi-Tech MT5634ZBA-USB modems . . . 411
Multi-Tech MT5634ZBA-V92 modems . . . 412
music-on-hold (MOH) . . . 414

N

Names/Number Template for Avaya Installation Wizard . . . 44
network integration . . . 85
network interface . . . 398

P

P330 LAN Expansion Module . . . 79
P333T-PWR power over Ethernet stackable switch . 356
paging equipment . . . 418
loudspeaker paging for G700 or G350 media gateways . . . 418
patch files
for IA770 . . . 219, 571
pinout chart
2-wire station . . . 336
Planning
documentation . . . 84
Logins . . . 707
S8300 Information . . . 711
Serial Numbers . . . 707
POE switches . . . 349
C360 . . . 349
C460 . . . 349
P333T-PWR . . . 349
power
AC . . . 107
AC Outlet Test . . . 107
Connecting . . . 109
DC . . . 110
Requirements . . . 107
Testing the AC Outlet . . . 107
power supplies
installation . . . 334
wiring . . . 334
power supplies for telephones
1151A1 -48V . . . 347
1151A2 -48V . . . 347
installing and wiring . . . 339
P333T-PWR . . . 356
power up . . . 109
Pre-installation Worksheet for Avaya Installation Wizard . . . 44
pre-upgrade service pack
activating . . . 239, 299, 591, 659
printers
connecting to a G700 or G350 Media Gateway . 395
Proxy Agent . . . 371

R

RAL 87
remaster command 258
Remote Feature Activation 85
Restricted Access Location 87
RJ-45 splitter for connecting two BRI stations 337

S

S8300
  B version 211, 563
  LEDs 81
S8700 Media Server 83
S8700/S8710 Media Server 83
safety instructions
  1151A1 and 1151A2 power supply 347
service pack
  for Communication Manager 218
service pack files
  for Communication Manager 570
Single Sign-On SSO
  RFA Single Sign-On 85
site verification 85
site-specific-option-number (sson) 177, 510
SNMP alarming on G700 511
stack 477, 528
stacks
  multiple units 99
supplementary ground conductor 87
switches
  adding new switch configuration 69
switch-to-call accounting link, testing 393

T

T1 DS1 span 396
task list 114, 424
  new G700 with S8700 . . . . . 117, 427
  upgrade G700 with S8300 . . . . 119, 121, 429, 431
  upgrade G700 with S8700 . . . . . 123, 433
Technical Specifications Table 701
Telephones
  connecting 333
telephones
  connectable 334
  installation 334
  wiring 334
telnet
  set parameters 138, 245, 446, 596
Terminal Configuration 372
terminal emulation
  ntt 73
  w2ktt 73
Terminal Emulator 372
terminal server 376
  administering IP services 388
  IOLAN+ 104 376
testing, switch-to-call accounting link 393
TFTP server
  on laptop 127, 213, 436, 565
TFTP server setup 188, 326, 524, 690
translations, CDR parameters 391

U

uninterruptible power supply 374
Unity CD 127, 436
Unity CD, access 213, 565
upgrade
  existing G700 without S8300
    manual procedures 687
  existing S8300A
    manual procedures 563
  existing S8300B
    manual procedures 639
  G700 with S8300 . . . . . 211, 279
    completing upgrade (S8300 primary controller) 277, 320, 636, 684
    configure G700 Media Gateway 314, 674
  G700 with S8700 323
    G700 firmware installation 331, 695
Upgrade Tool for LSP/G700 45
UPS 374
USB CD-ROM drive 127, 213, 436, 565

V

Voice Announcement over LAN Manager 373

W

wiring
  2-wire digital station 335
  alarm 335
  analog station 335
  CO trunk 335
  DID trunk 335
wiring diagram
  DC 111
wiring telephone power supplies
  procedures 339

X

X330 WAN Access Routing Module 79
X330STK Stacking Sub-Module
  installation 98